# INCOGNITO CONSUMER HARM

*Yunsieg P. Kim*[*]

104 WASHINGTON UNIVERSITY LAW REVIEW __ (forthcoming 2026)

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 designed 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 app quietly retains photo IDs it promised to delete. Because consumers cannot readily detect these harms, the law's ordinary enforcement triggers rarely fire: victims do not complain, lawyers are not retained, and regulators receive no report. Thus, discovery of incognito consumer harm depends more on leaks, hacks, whistleblowers, and other accidents than on routine enforcement mechanisms.

Incognito consumer harm matters for three reasons. First, it exposes a structural weakness in U.S. consumer protection. Both public and private enforcement depend on the victims' awareness, but courts cannot litigate the invisible and agencies do not routinely audit products for concealed design choices. Second, it highlights a diagnosis-cure mismatch in the literature. Even when scholars describe "invisible" harms, they often propose remedies that assume detection, such as procedural reforms, bans, and enhanced damages, even though incognito harm is designed precisely to prevent detection. Third, modern technology makes concealment scalable, continuous, and embedded in everyday products. As AI increases firms' appetite for granular and intimate data, the payoff to undiscoverable extraction only grows.

This Article argues that incognito consumer harm requires fundamental reform, not marginal tweaks, because existing law fails doubly. It is not built to surface invisible injuries and, even when misconduct is exposed, doctrine often fails to recognize concealed risk, loss of control, and informational deprivation as cognizable harms. Without detection-first reform, the status quo persists. We learn about hidden misconduct only when systems are breached or insiders come forward—in effect, relying on wrongdoers to expose wrongdoing.

*Keywords: Civil litigation, Tech law, Access to justice, Law & economics*

---

[*] 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.

## INTRODUCTION

How can the law punish wrongdoing if most victims never realize that they were harmed? This uncomfortable question frames the problem of incognito consumer harm, wherein companies deliberately design misconduct to remain unnoticed by most victims. A robot vacuum cleaner covertly records video inside private homes, under the pretense of mapping rooms for better cleaning.[1] Honey, a browser extension that claims to "automatically . . . apply[] coupon codes," records everything a user does with precise timestamps—including when the user "went looking for an Airbnb in Berlin . . . for two adults for the period from March 04 to March 05" and which video the user watched on a streaming service.[2] Tea, a popular dating app, requested users' photo IDs to verify identity and promised to delete the information after verification, but quietly retained it.[3] In each case, consumers have little or no way to detect the harm on their own. Thus, incognito consumer harm short-circuits the usual triggers of enforcement: victims cannot sue or report because they do not know that they were wronged. Without an accident or whistleblower to reveal the scheme, the law remains oblivious while harm continues unabated. In the case of the dating app Tea, for instance, the harm came to light only after hackers breached its servers and exposed the supposedly deleted personal information.[4] In short, we live in a world where we rely on wrongdoers to expose other wrongdoers' wrongdoing.

While harming unsuspecting victims in itself is not new, three traits of incognito consumer harm make it novel and formidable, and thus noteworthy. First, incognito harm exposes a structural flaw in the U.S. legal system: the system's dependence on victim awareness to trigger enforcement. U.S. consumer protection law is often framed as a mix of public and private enforcement, in which agencies police unfair and deceptive practices while private plaintiffs

---

[1] Julian Fell, *Insecure Deebot Robot Vacuums Collect Photos and Audio to Train AI*, AUS. BROADCASTING CORP. (Oct. 4, 2024), *available at* https://www.abc.net.au/news/2024-10-05/robot-vacuum-deebot-ecovacs-photos-ai/104416632.

[2] *More Than Just Coupon Codes: Browser Extension Honey Also Collects Their User's History Data*, DATAREQUESTS.ORG, https://www.datarequests.org/blog/honey-data-collection/ ("The free browser extension 'Honey' wants to save their users money by automatically finding and applying coupon codes. . . . [But] Honey collects history data on a large scale, contrary to what their own privacy policy says. . . . Honey knows . . . . on March 23 at 5 PM, [a user] watched the documentary 'Scanning The Pyramids' via the streaming provider CuriosityStream").

[3] 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) ("[A]bout 13,000 selfies and images of identification documents, which the [dating app] solicited to verify that users are women" belonging to "users who signed up before February 2024" were stolen, despite "Tea's privacy policy [stating that] the selfies it solicits are deleted shortly after users are verified"), *available at* https://www.nytimes.com/2025/07/26/us/tea-safety-dating-app-hack.html.

[4] *See id*. ("According to Tea's privacy policy, the selfies it solicits are deleted shortly after users are verified" but "[t]he hacked images were not deleted.").

sue under statutes and common law.[5] In practice, however, courts do not litigate the invisible and agencies do not routinely audit every consumer product for concealed design choices. The system is therefore conditional, in that it works best for conspicuous harms that are immediate, legible, and traceable. Incognito consumer harm evades these conventionally assumed detection mechanisms.

The result is not marginal under-enforcement but practical impunity of the system at the very outset. Complaint-driven triggers never fire. Unlawful business practices go unchallenged, and even flourish, because they are never identified. The law's perspective of consumer harm becomes systematically biased because it sees only the harms it detects and mistakes that conspicuous subset for the whole.[6] The larger universe of undetected injuries remains unaccounted for and functionally ungoverned. What good is a legal system built for visible injuries in a world where injury is designed to be invisible?

The second defining feature of incognito consumer harm is that it reveals a diagnosis-cure mismatch in the literature. Scholars increasingly recognize that modern consumer harms—mediated by algorithms, opaque systems, and pervasive data collection—can be hard to perceive. Yet, even when they label harms "invisible," they often propose solutions that require the harm to first be detected. For example, Professor Mark Lemley proposes regulating certain exploitative data practices that consumers rarely detect, without specifying how regulators would uncover such practices in the first place.[7] Professor Andrew Miller proposes litigation reforms for "invisible" algorithmic profiling,[8] but this presupposes plaintiffs who discover the harm and sue, which is precisely what incognito harm is designed to prevent. Put differently, many works treat incognito harm as a remedial problem when it is first a detection problem. Promises of compensation and deterrence are hollow if wrongdoing never triggers enforcement. In too many cases, the most after-the-fact fixes can do is to perversely rely on accidents, data leaks, or hacks to reveal the misconduct.

---

[5] *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.").

[6] *See infra* Part II, Section C.

[7] *See* Mark A. Lemley, *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).

[8] Andrew Miller, *Invisible Allies: Algorithmic Consumer Profiling and the Rise of New Group Harms*, __ YALE J. L. & TECH. 45 (2026) (proposing "aggregate litigation" as a solution).

Third, incognito consumer harm differs from older forms of unnoticed injury because modern technology makes concealment scalable and woven into everyday products. Technology did not invent concealment, but it allows it to run continuously, remotely, and automatically across millions of consumers. Today's consumer economy is dense with sensors, intermediaries, and black boxes.[9] Many devices go further and collect intimate data as a condition of use. In 2025, Facebook rolled out a feature that appears to scan private photos stored in users' phones to improve its AI.[10] The broader point is that, whatever the consent mechanics in any interface, large-scale ingestion of private consumer data is now technically feasible and the boundary between "functionality" and "extraction" is blurring. Yet, too many practitioners and academics dismiss technologically enhanced phenomena as a distinction without a difference, treating technology as something that just accelerates what can be done "by a human using a pen and paper."[11] But scale alone can make phenomena genuinely different: it is technology that enabled a "tiny middleman" to intercept a "million messages" carrying passcodes for Signal and WhatsApp accounts in a month.[12]

Incognito consumer harm is especially dangerous because the incentives to commit it are broad and growing. As AI training consumes vast amounts of data and publicly available sources of high-quality data run out,[13] firms face increasing pressure to find new sources of granular and intimate information

---

[9] *See, e.g.*, Sylvia Lu, Note, *Data Privacy, Human Rights, and Algorithmic Opacity*, 110 CAL. L. REV. 2087, 2120 (2022) (AI-driven consumer tools operate as opaque "black box" systems that invisibly monitor and decide, thus hindering oversight).

[10] Gretchen Oestreicher, *How to Turn Off Meta AI: Facebook, Instagram, and WhatsApp*, METRICOOL (July 8, 2025) ("As of May 27, 2025, EU users can no longer turn off Meta AI to prevent it from reading and learning from their data"); *id*. (the button to block Meta from "uploading [photos] from your device to Meta's servers" is "[g]et creative ideas made for you by allowing camera roll cloud processing."), https://metricool.com/opt-out-meta-ai-training/.

[11] *Cf.* Ericsson Inc. v. TCL Communications Technology Holdings Ltd., 955 F.3d 1317, 1327 (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"); *see also* Thibault Schrepel, *The Fundamental Unimportance of Algorithmic Collusion for Antitrust Law*, JOLT DIGEST (Feb. 7, 2020) (citing Thibault Schrepel, *Collusion by Blockchain and Smart Contracts*, 33 HARV. J. L & TECH. 117 (2019)) (claiming that 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.").

[12] Ryan Gallagher, Crofton Black & Gabriel Geiger, *How a Tiny Middleman Could Access Two-Factor Login Codes from Tech Giants*, BLOOMBERG (June 16, 2025) (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."), *available at* https://www.bloomberg.com/news/articles/2025-06-16/two-factor-authentication-codes-take-insecure-path-to-users.

[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.

tied directly to identifiable individuals. That pressure cuts across industries, as any firm that can monetize data has reason to push extraction further while concealing it.[14] Separate from technological development, fundamental changes in consumer behavior itself—among them a phenomenon called "brandless shopping"[15]—are incentivizing the commission of incognito consumer harm even further. In this environment, incognito consumer harm is not merely the work of a few bad actors but a near-universal strategy: harvest what consumers cannot see, because what they cannot see, they cannot even think to challenge.

This Article argues that incognito consumer harm demands fundamental reform, not the marginal tweaks within existing law commonly advanced in the current literature.[16] The problem is not a small mismatch between new harms and old rules, but a structural failure of the enforcement model in two respects. First, existing law is not designed to detect invisible injuries. Litigation and regulation largely depend on victims or the public to notice harm and sound the alarm, an assumption that collapses when harm is engineered to evade notice. Second, even when incognito harm is exposed—by a hack, a whistleblower, or sheer accident—existing law often lacks the vocabulary to treat it as a cognizable injury and provide redress, especially when the harm is concealed risk, loss of control, or informational deprivation rather than immediate physical or monetary loss. The claim is not only that hidden harms are increasing, but also that a system built for visible injuries will systematically fail in a world of engineered invisibility. The solution requires detection-first consumer protection and legal recognition of injuries even when they are, by design, initially unseen.

This Article proceeds in three parts. Part I defines incognito consumer harm and delineates its scope. It presents a working definition (consumer-facing wrongdoing designed not to be noticed by most victims) and develops a taxonomy that distinguishes fully incognito from partially incognito harms, and intentional concealment from negligent invisibility. The point is not mere wordplay. The point is to show, concretely, what the legal system is currently structured not to see—and why incognito harm is not confined to privacy, but extends to any consumer injury deliberately kept secret from those affected.

---

[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* Part I, Section D.

[16] *See, e.g.*, Lemley, *supra* note 7 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).

Part II explains why existing legal frameworks fail even when we know what incognito consumer harm looks like. First, invisibility erodes the detection mechanisms of law: both litigation and regulation assume that victims will notice harm and trigger enforcement, but consumer protection remains largely complaint-driven and ill-suited to harm designed to evade detection. Second, even when incognito harms are eventually uncovered, current law often struggles to recognize or articulate them as legally cognizable injuries. The law's weak detection mechanism and narrow definition of injury create a survivorship bias, forcing the law to see only visible harms and mistake that subset for the full universe of consumer harm. Part III proposes reforms that match the problem's structure: detection-first strategies (audits, whistleblower incentives, and built-in monitoring) and tools that penalize concealment and enable targeted information-forcing. I conclude by stressing the need to treat concealment itself as sanctionable, in a world where consumer consent is increasingly fictional and AI is fueling unprecedented appetite for data. Without fundamental reform, the race to the bottom will continue, harming as many consumers as possible before detection and undermining the already dwindling trust in free markets.

## I. DEFINING INCOGNITO CONSUMER HARM: CONCEPT AND SCOPE

An obvious question for any phenomenon with a new name is whether the problem is truly novel enough to merit the name. After all, harming victims unaware, in itself, is not new. A corporation might secretly dump toxic waste in a water source, harming anyone who drinks from it over years or decades 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] In each instance, the injury initially (sometimes, even permanently) escapes the notice of most victims. So, what distinguishes incognito consumer harm as a concept warranting its own label?

The first distinctive and underappreciated feature of incognito consumer harm is that technology has scaled and accelerated even old, familiar kinds of consumer-facing misconduct into a qualitatively new problem. We have long

---

[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) (renters are often unaware of unlawfully deregulation, so they do not challenge 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) ("victims of medical malpractice . . . may be unaware for many years that they have been injured tortiously . . . .").

known that speed and scale can transform an activity. Superficially, the printing press only mechanized the manual task of copying books.[20] But that innovation, by radically reducing the cost and time needed to produce books, revolutionized society by breaking the intelligentsia's "monopoly over common knowledge."[21] Today, digital tools let firms inflict covert harm on thousands or even millions at the push of a button,[22] thereby making incognito consumer harm a form of technology-assisted ambush: harder to anticipate, harder to detect, and thus far more formidable its analog predecessors. Yet, law often treats faster execution as legally irrelevant. Scholars dismiss algorithmically accelerated wrongdoing as "old wine in new bottles" even when automation collapses a lengthy process into 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]

The second distinguishing feature of incognito consumer harm is that scholars tend to focus on *what* the harm is, while neglecting *how* it is concealed. Although some have discussed and even taxonomized technology-assisted harms that operate outside consumers' knowledge, the literature has not classified these harms by (1) the degree of invisibility and (2) the culpability behind that invisibility. For instance, FTC Commissioner Rebecca Slaughter has written what she calls "a baseline taxonomy of algorithmic harms," which she recognizes are generally invisible to consumers because algorithms often give a "false impression that these problems do not . . . exist."[25] But Slaughter's taxonomy tracks sources of harm—bad input data, flawed interpretations of outputs, and inadequate testing—rather than the mechanisms that keep the harm hidden.[26] That focus, while useful, is incomplete, as knowing what the harm looks like is of limited practical value if we cannot tell when it occurs. The absence of a concealment-centered framework also makes it harder to craft solutions tailored to the many ways that wrongdoers keep harm invisible to evade detection. To address this gap, Part I defines the concept of incognito consumer harm and illustrates its scope, in order to ground the theoretical and normative discussion that follows.

---

[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 . . . . [g]enerally, reproduction 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).

[22] *See* Gallagher, Black & Geiger, *supra* note 12.

[23] *See* Schrepel, *supra* note 11.

[24] *See Ericsson*, 955 F.3d at 1327.

[25] 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. 1, 1 (2021).

[26] *See id*. at 7-21.

### *A. Definition and Core Examples*

Incognito consumer harm refers to consumer-facing harm intentionally designed go unnoticed by most victims, so that it bypasses the ordinary channels of awareness, complaint, and redress. 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 app, asked users to submit selfies and photo IDs to verify identity and promised to delete the data after verification, but quietly retained the data for years.[27] Honey, a PayPal-owned browser extension that claims to find the best discounts for online shopping, recorded virtually everything users did online.[28] 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 only by accident. Tea's deception surfaced only after hackers breached its servers and exposed the supposedly deleted photos and IDs,[29] 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.[30]

Notably, incognito consumer harm is not limited to data and privacy. A wide range of consumer injuries intentionally kept secret from the victims can qualify, from social media influencers promoting a product without disclosing that it is paid advertising[31] to traditional harms like landlords illegally raising rent.[32] Across various contexts, the wrongdoer's strategy is the same: preserve the victim's obliviousness. This Article emphasizes data-privacy examples of incognito consumer harm because they highlight two major gaps in the literature. First, scholars often treat technology-enhanced incognito consumer harm as mere acceleration of old misconduct, and thus a distinction without a difference from old misconduct, even though technology-assisted scaling and automation make it incomparably more formidable.[33] Second, scholars focus on the harm at the expense of concealment of the harm, even as technology multiplies both the means and efficacy of hiding harm far beyond what was once imaginable.[34]

---

[27] *See* Kwai, *supra* note 3.

[28] *See* DATAREQUESTS.ORG, *supra* note 2.

[29] *See* Kwai, *supra* note 3.

[30] MegaLag, *Exposing Honey's Evil Business Model*, YOUTUBE (Dec. 22, 2025), https://www.youtube.com/watch?v=wwB3FmbcC88.

[31] *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, 165 (2024) (many consumers are misled into thinking "that paid content is unpaid").

[32] *See* La Mort, *supra* note 18.

[33] *See supra* note 11 and accompanying discussion.

[34] *See supra* notes 20-21 and accompanying discussion.

It is important to distinguish incognito consumer harm from concepts like diffuse or delayed harm. Diffuse harm—say, a hidden monthly fee of 61 cents on millions of consumers[35]—is characterized by each individual injury being so small that many victims may notice but do not care to complain. Incognito consumer harm, by contrast, can impose substantial per-person injury because perpetrators rely on victims never realizing what was taken or compromised: invisibility lets firms extract significant money or data from each consumer without provoking pushback. Incognito harm also differs from latent injuries that surface years later (like toxic exposure) in that, even if delayed, the victim eventually experiences symptoms or losses.[36] Incognito harm is designed to remain concealed indefinitely unless an external rupture—a whistleblower, malicious data hack, or investigative discovery—reveals it. Its defining feature is engineered invisibility, which short-circuits the legal system's usual triggers: when victims never know they were wronged, complaint-driven enforcement and other visible red flags never activate. With the concept clarified, I proceed to categorize incognito consumer harm according to visibility and intent.

### *B. Categories of Incognito Consumer Harm: Visibility and Intent*

Incognito consumer harms are not uniform. They vary along two key dimensions: first, degree of invisibility (fully vs. partially invisible) and second, nature of concealment (intentional deception vs. negligent failure to inform). These distinctions are not merely academic, but instead bear directly on how we should detect, deter, and punish such wrongdoing. Fully concealed harms require different detection strategies from harms that *sometimes* surface, and deliberate cover-ups warrant greater culpability than wrongdoing concealed by mere neglect or oversight. This section outlines each category of harm in turn, and explains why these differences matter for legal doctrine and enforcement.

#### 1. Fully vs. Partially Invisible Harms

Some misconduct is fully incognito, as no consumer is likely to discover it absent an extraordinary fluke, a whistleblower, or a breach, the classic case being privacy violations engineered to leave victims none the wiser. I have

---

[35] Jon Brodkin, *AT&T Sued Over Hidden Fee That Raises Mobile Prices Above Advertised Rate*, ARS TECHINCA (June 24, 2019) (junk fee started at 61 cents per month and became $1.99 per month, at which point a class action was brought), https://arstechnica.com/tech-policy/2019/06/att-sued-over-hidden-fee-that-raises-mobile-prices-above-advertised-rate/.

[36] *See, e.g.*, Paul D. 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.").

already discussed examples involving robot vacuum cleaners, the dating app Tea, and the Honey browser extension collecting sensitive data.[37] Consumers typically cannot detect these invasions themselves. In fully incognito schemes, victims have no practical trigger to complain, so the harm stays hidden unless a malicious outsider or whistleblowing insider forces it into public view.[38]

Other incognito consumer harms are *partially* hidden, as they are not apparent to most victims but discoverable in unusual circumstances. A small subset of consumers or an unlikely chain of events may bring the harm to light while the majority remain oblivious. For instance, algorithmic manipulation or discrimination can affect thousands unaware, but a researcher, journalist, or whistleblower who talks to a broad enough group 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.[39] 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 charge different prices depending on which computer they used to access the 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.[40] Beyond this example, scholars argue that sophisticated algorithmic targeting can create "invisible" classes of disadvantaged consumers who never realize they are being profiled.[41] In such contexts or settings, the probability of discovery is low but not zero.

This visibility spectrum matters because even *partially* hidden harms undermine the existing enforcement model's core assumption that victims will notice injuries and come forward.[42] Some scholars point to aggregate litigation as the answer for partially hidden harms like algorithmic discrimination.[43] In theory, a single aware victim could file a class action and the notice process

---

[37] *See supra* notes 1-4 and accompanying discussion.

[38] *See supra* notes 4, 30 and accompanying discussion.

[39] Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882.

[40] *Id*.

[41] Miller, *supra* note 8, at 3.

[42] *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) ("private enforcement of . . . consumer protection statutes [is] a strong deterrent against deceptive business practices").

[43] *See, e.g.*, Miller, *supra* note 8, at 45; Daniel Wilf-Townsend, *Artificial Intelligence and Aggregate Litigation*, 103 WASH. U. L. REV. __ (2026) ("AI tools can create harms that are only demonstrable at the level of an affected group, which is likely to frustrate traditional individual claims. Aggregation creates opportunities to prove harm . . . at the group level.").

would alert the rest. But in practice, a few people noticing is unlikely to trigger enforcement because most consumers do not sue even when they know they were harmed, as "litigation is seldom worth the trouble."[44] This is especially likely for low dollar amount injuries which are the most typical of algorithmic price discrimination, such as purchases of groceries or "a bag of dog food."[45]

One may respond that low-dollar injuries are precisely what class actions are for. As Judge Posner quipped, "only a lunatic or a fanatic sues for $30,"[46] which is why class actions aggregate many $30-claims into a case worth bringing. But aggregation helps only after someone files suit. Class actions are of little use when most victims never notice the harm and the few who do are unlikely to act. As a result, even partially visible incognito harm can be functionally invisible to the legal system, making reactive enforcement inadequate. Reform must move detection upstream and tailor tools to visibility: proactive oversight for fully invisible wrongdoing, and stronger reporting channels and incentives for early discovery for partially visible harms, which Part III explores in depth.

2. Intentional v. Negligent Concealment

Incognito consumer harm also varies by the perpetrator's state of mind behind the concealment. Invisibility is often intentional. 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.[47] A form of knowing concealment short of outright falsification is deception by obfuscation. For example, Meta suggests to 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.[48]

In contrast, some harms are incognito through negligence. A company did not *aim* to hide the injury, but its lack of care resulted in consumers never

---

[44] *See* James M. Treece, *Trademark Licensing and Vertical Restraints in Franchising Arrangements*, 116 U. PA. L. REV. 435, 444 n.12 (1968) ("[N]umber of reported cases" likely underreports consumer harm "because litigation is seldom worth the trouble" to consumers).

[45] Miller, *supra* note 8, at 15, 24.

[46] Carnegie v. Household Int'l, Inc., 376 F.3d 656, 661 (7th Cir. 2004) ("The realistic alternative to a class action is not 17 million individual suits, but zero individual suits, as only a lunatic or a fanatic sues for $30.").

[47] *See Google: AG Rosenblum Announces Largest AG Consumer Privacy Settlement in U.S. History*, OREGON DEPT. OF JUSTICE (Nov. 14, 2022), https://www.doj.state.or.us/media-home/news-media-releases/largest-ag-consumer-privacy-settlement-in-u-s-history.

[48] *See* Oestreicher, *supra* note 10.

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 50 million consumers were stolen after a hacker found "an unprotected router" in T-Mobile's network.[49] 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 voluntarily claimed responsibility for the hack by giving an interview to the Wall Street Journal.[50]

These distinctions in intent matter for several reasons. First, from an enforcement and policy standpoint, the law typically calibrates penalties to the actor's level of fault.[51] Without differentiation, firms would have no incentive to choose transparency or invest in compliance. If negligent omissions drew the same punishment as deliberate fraud, a bad actor might reason that it might as well *intentionally* hide its misdeeds. Conversely, a firm that made a good-faith error (say, a one-time failure to send a required notice) might deserve a chance to fix the issue and avoid the maximal sanction reserved for schemers. Many areas of law reflect this principle in practice. For example, privacy statutes often impose only modest liability for negligent violations but allow punitive damages or higher fines for willful violations.[52] Tort law, too, limits punitive damages to conduct that is more than merely negligent, like intentional or recklessly indifferent wrongdoing.[53] Incognito harms should be no different.

Second, the intent behind concealment can influence the doctrinal tools available to address concealment. Some causes of action require intent: fraud,

---

[49] *See* Jonathan Stempel & Sara Merken, *T-Mobile to Pay $350 Mln in Settlement Over Massive Hacking*, REUTERS (July 23, 2022), https://www.reuters.com/business/media-telecom/t-mobile-pay-350-mln-settlement-over-massive-hacking-2022-07-22/.

[50] *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), https://www.wsj.com/business/telecom/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105.

[51] *Cf.* Justin V. Rodriguez, Note, *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.").

[52] *See, e.g.*, Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47, 52 (2007) (Under 15 U.S.C. § 1681n(a), "Anyone who 'willfully fails' to provide notice is civilly liable to the consumer.").

[53] *See, e.g.*, Wauchop 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.").

for instance, requires knowing misrepresentation.[54] If a harm was intentionally concealed, it may enable fraud claims or willful violation penalties, whereas negligent concealment may fall under failure-to-warn or simple negligence.[55] Intentional incognito harms may also justify shifting burdens or presumptions in litigation. For example, if a court finds that a company deliberately concealed evidence of a defect, it might infer that any doubt about causation or harm should be resolved in the plaintiffs' favor, analogous to how courts handle intentional spoliation of evidence.[56] Negligent concealment, on the other hand, might not trigger such doctrinal leeway, but still violate consumer protection statutes or regulations that impose a duty to disclose material information.[57]

Finally, intent is directly relevant to normative culpability and public trust. Intentional concealment represents a breach of basic trust and calculated betrayal of consumers. The perpetrator knows that it is harming consumers and chooses to hide it, which justifies greater condemnation and potentially different remedies, such as punitive damages, disgorgement, or even criminal liability in egregious cases. Negligent incognito harms, though still serious, are more plausibly framed as failures of diligence or competence—harms to be corrected and compensated for without the same moral judgment. This distinction should shape how legal responses are designed. Enforcement resources might be focused on the worst actors who engineer concealment, and reforms can be tailored so as not to over-deter businesses from self-reporting problems. For instance, regulators might impose stiff fines when evidence shows a purposeful cover-up, but treat tardy self-disclosure more leniently when the invisibility stemmed from negligence and the implicated firm comes forward voluntarily.

In sum, parsing incognito harms by visibility and intent clarifies why they are uniquely difficult. Fully invisible harms engineered for secrecy present a near-impenetrable challenge for traditional enforcement, like a tree falling in a forest with no one to hear, while partially invisible harms can still exploit limited consumer awareness and persist for long periods. Moreover, intentional concealment is a fundamentally different wrong from negligent omission: the

---

[54] *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.'").

[55] *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).

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

[57] *Cf.* Collins v. Throckmorton, 425 A.2d 146, 150 (Del. 1980) ("We . . . recognize the general rule that, where a litigant intentionally suppresses or destroys pertinent evidence, an inference arises that such evidence would be unfavorable to his case.").

former attacks the transparency on which markets and law depend, while the latter reflects a breakdown of corporate responsibility. Because the solutions and sanctions must differ, these categories do more than refine terminology. Instead, they set up this Article's central prescriptions: detection-first tools for fully incognito consumer harms and a direct legal reckoning with concealment itself for intentional schemes. 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*

Incognito consumer harm flourishes in the gaps of incomplete consumer contracts. Incomplete contracts themselves are not new, as 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.[58] As also noted by scholars, the same problem continues to render consumer consent a thing of fiction, as boilerplate terms routinely gloss over what firms actually do with consumer assets like data, attention, and trust.[59] 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.[60] The result is a mass incomplete consumer contract scenario ripe for exploitation.

What makes the contemporary imbalance especially pernicious is that the information asymmetry now flummoxes not only lay consumers, but also the experts meant to police it, such as judges, lawyers, and regulators. Digital products are designed to be intuitive, which can lull 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."[61] This illusion of proficiency leads legal professionals to overestimate their grasp of complex digital systems without apprehending the novel risks and failure modes that these tools introduce. Federal courts assume that an email functions

---

[58] *See, e.g.*, W. David Slawson, *Mass Contracts: Lawful Fraud in California*, 48 S. CAL. L. REV. 1, 1 (1974), *available at* HeinOnline.

[59] *See, e.g.*, Lemley, *supra* note 7 at 249 ("Even where privacy laws offer a nominal choice, companies circumvent it by making the sharing of data the easier option.").

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

[61] Yunsieg P. Kim, *The Faster Horse Fallacy: How the Law Idealizes Technology*, 2025 U. ILL. L. REV. 609, 613 (2025).

just like a letter, only faster and cheaper, even though companies abuse spam filters to avoid making required notices.[62] Scholars present technology-assisted discovery tools as "almost certainly better than humans in precision," even though AI can make errors that human lawyers are highly unlikely to make.[63]

This misalignment leaves legal experts with a dangerous blind spot, breeding 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 industry's good faith. The result is a paper shield: a regulation that looks strict on its face but is toothless against hidden misconduct. One example is the wave of online age-verification laws since 2020. Many of these require platforms to collect a user's ID for age checks and then purge that sensitive data immediately, to prevent misuse. But without audits, enforcement relies entirely on trust—and "even if the law doesn't impose" specific retention mandates, one must "trust that companies will actually delete" the data as promised, a premise which a federal court called "dubious."[64] Another example is New York's Algorithmic Pricing Disclosure Act, enacted on July 8, 2025, which requires "[a]ny entity that sets the price of a specific good or service using personalized algorithmic pricing" to give consumers a "clear and conspicuous disclosure,"[65] and authorizes enforcement proceedings when the attorney general has a "reason to believe" that a violation has occurred.[66] However, the law provides no mechanism to detect whether companies are using algorithms or personal data to set prices.

Modern mass contracts mix incomplete agreements with technological opacity in a way that is uniquely perilous for consumers. Information asymmetry, once largely a matter of fine print and hidden fees, has been supercharged by digital complexity to the point that even courts and regulators often struggle to discern what is happening. Consumers become bound by contractual and technical constraints they neither understood nor meaningfully accepted, while firms profit from that knowledge gap. And when legal actors treat new systems as mere incremental updates, they risk addressing only the visible symptoms rather than the code- and design-level mechanisms that generate incognito harm.

---

[62] *Id*. at 613-635.

[63] *Id*. at 642-650 (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)).

[64] *See* Free Speech Coal., Inc. v. Colmenero, 689 F. Supp. 3d 373 (W.D. Tex. 2023), *aff'd in part*, Free Speech Coal., Inc. v. Paxton, 95 F.4th 263 (5th Cir. 2024), *aff'd*, 606 U.S. 461 (2025) (the premise that readers will "trust that companies will actually delete" their authentication data is "dubious").

[65] N.Y. Gen. Bus. Law § 349-a, at 2.

[66] *Id*. at 4 (authorizing the attorney general to send cease-and-desist letters and to apply for an injunction, and authorizing state courts to issue injunctions and civil penalties).

### *D. A 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 identity from consumers. Historically, the need for brand recognition kept firms visible and tethered to accountability because corporate survival depended on being known and trusted by customers, which inherently limited the extent to which a firm could hide ongoing malfeasance.[67] 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.[68] 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. Should the brandless retail model continue to proliferate, the law's present focus on conspicuous, brand-linked wrongdoing will be looking at an ever-shrinking tip of the iceberg, while a growing mass of incognito misconduct remains submerged and unaddressed.

Although brandless shopping seems to have escaped the notice of legal scholars,[69] 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"[70] 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:

---

[67] *Cf.* MARK BATEY, BRAND MEANING: MEANING, MYTH, AND MYSTIQUE IN TODAY'S BRANDS 2 (2008) ("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.").

[68] Juozas Kaziukénas, *Amazon Laid the Brandless Foundation for Temu*, MARKETPLACE PULSE (Oct. 10, 2024) ("Amazon is a brandless retailer. Most shoppers do not include a brand name in their searches (they look for 'running shoes' rather than 'Nike running shoes'), and most products carry a brand name shoppers have never seen before."), *available at* https://www.marketplacepulse.com/articles/amazon-laid-the-brandless-foundation-for-temu.

[69] 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 (10 entries under the category "key number") were all irrelevant to brandless shopping.

[70] 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.


XYKEEY Set of 2 Toothpaste Squeezer Rollers, Metal Toothpaste Tube Wringer Seat Holder Stand (Stainless Steel)

4.6 ★★★★½ 12,513 ratings

Amazon's Choice

**6K+ bought** in past month

$9.99 ($5.00 / Count)

prime One-Day
FREE Returns

Get a $50 Gift Card for each friend who is approved for Prime Visa or Amazon Visa. Earn up to $500 each year. **Find out how**

Color: **Stainless Steel**

71


Toothpaste Squeezer - Metal Tube Squeezer Stainless Steel Tube Wringer UDQYQ Toothpaste seat Holder Stand (Silver)

4.6 ★★★★½ 2,366 ratings |
Search this page

**700+ bought** in past month

$9.99 ($5.00 / Count)

prime One-Day
FREE Returns

72

In this environment, branding becomes fluid or irrelevant, making it that much harder for buyers to even identify who they are transacting with, let alone hold any specific seller accountable if something goes wrong. In theory, this brandless model need not jeopardize consumers if a trusted intermediary takes the specific brand's place. Many shoppers effectively substitute Amazon's brand (and the supposed integrity of its customer review system) for the myriad unknown brands on its platform, assuming that high ratings and Amazon's

---

[71] *XYKEEY Set of 2 Toothpaste Squeezer Rollers, metal Toothpaste Tube Wringer Seat Holder Stand (Stainless Steel)*, AMAZON (last visited July 13, 2025), https://www.amazon.com/Toothpaste-Tube-Squeezer-Rollers-Wringer/dp/B07SHL6P8V/?th=1 [https://perma.cc/JQ85-HGXM].

[72] *Toothpaste Squeezer - Metal Tube Squeezer Stainless Steel Tube Wringer UDQYQ Toothpaste seat Holder Stand (Silver)*, AMAZON (last visited July 13, 2025), https://www.amazon.com/Toothpaste-Squeezer-Stainless-Wringer-Holder/dp/B085W1ZSBT/ [https://perma.cc/5BZV-VF3Q].

overall reputation ensure a baseline of quality and safety. Ideally, the platform itself would serve as a kind of meta-brand, vetting third-party products and policing fraud so that users can safely ignore who the underlying seller is.[73]

In practice, however, Amazon's gatekeeping has been alarmingly porous. Studies estimate that roughly 42% of the 720 million Amazon product reviews posted in 2020 were fake or manipulated,[74] calling into question the reliability of the very ratings consumers rely upon. Even blatantly substandard or unsafe merchandise can maintain a glowing rating. For instance, third-party sellers have offered electrical fuses and connectors that boast 4.5-star average reviews despite failing to meet the entire point of a fuse or connector, such as actually preventing electrical overloads to avoid fires or electrocution.[75] Such problems suggest that neither Amazon's brand name nor its review system is effectively performing the quality-assurance role that the brandless model presupposes.

Platforms not only struggle to police bad actors, but they sometimes appear to tolerate or even enable them. Consumer advocates have documented allegedly fraudulent or dangerous products remaining on Amazon long after being flagged, while sellers of banned items often resurface under new aliases. For example, nutritional supplements containing less than 2% of the advertised active ingredient have been observed.[76] In another case, a banned seller allegedly relisted the same product under a new name with barely altered packaging, with the old brand name simply blurred out.[77] Paid-review fraud is similarly persistent. Although Amazon bans it, customers regularly report being offered

---

[73] Kaziukénas, *supra* note 68.

[74] *Blumental Calls on Amazon to Curb Rampant Fraudulent Reviews*, RICHARD BLUMENTHAL, U.S. SENATOR FOR CONNECTICUT (Dec. 5, 2022), *available at* https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-cals-on-amazon-to-curb-rampant-fraudulent-reviews.

[75] Louis Rossmann, *Amazon Sells Dangerous Electrical Crimps*, YOUTUBE (Dec. 16, 2023), https://www.youtube.com/watch?v=y83BS_mK9GE; Louis Rossmann, *Amazon Sells Fake Electrical Fuses*, YOUTUBE (Dec. 30, 2023), https://www.youtube.com/watch?v=B90_SNNbcoU.

[76] Hank Schultz, *9 of 10 Amazon Galantine 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-; *see also* Marielle Segarra, *Counterfeit Goods Sold Online Can Be Dangerous. Here's How to Avoid Getting Duped*, NPR (Oct. 26, 2024) (many drugs sold on Amazon have little to no active ingredients"), https://www.npr.org/2024/10/26/nx-s1-5163453/how-to-avoid-buying-counterfeit-products-red-flags.

[77] 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.

cash or gift cards for five-star ratings.[78] Meanwhile, Amazon has leaned further into the "race to the ultracheap brandless bottom" with "Haul," a discount storefront that "looks like a Temu version of Temu"[79] and sells brandless products such as "$1 earrings and $8 leggings."[80] The result is an even more permissive environment for incognito consumer harms to incubate and fester.

This phenomenon is not limited to Amazon. The race to the bottom in online retail only appears to be accelerating across the industry. Between September 2022 and January 2024, Amazon reportedly lost 2.6 million U.S. users while Chinese competitor Temu, an online shopping platform notorious for rock-bottom prices and no-name merchandise, gained an astonishing 51.4 million users in the same period.[81] In other words, consumers are flocking to platforms where anonymity and minimal oversight are not flaws but selling points. As this shift continues, an ever-greater share of consumer transactions will involve ephemeral sellers that have no brand or reputation to defend and can easily evade consequences. The practical result is a world where finding a responsible party to blame or sue becomes exceedingly difficult, and where traditional notions of deterrence through brand accountability break down. It poses a stark challenge for consumer protection: how can the law trace and deter wrongdoing when neither the harm nor the perpetrator wants to be seen?

The takeaway is humility and vigilance. The way technology presents itself—frictionless and familiar—can mask how it actually operates and how quickly it evolves beyond the law's view, aided further by changing 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 rather than assume it. Until then, complexity and asymmetry will continue producing harms hidden in plain sight. Closing the gap will require clearer disclosures, greater technological literacy in law, and more adaptive, detection-first regulatory strategies. 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.

---

[78] 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), 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/.

[79] Katie Notopoulos, *Amazon's New Discount Section, 'Haul,' Looks Like a Temu Version of Temu*, BUS. INSIDER (Nov. 14, 2024), https://www.businessinsider.com/amazon-haul-temu-shein-compared-which-is-better-worse-2024-11.

[80] Jason Del Ray, *Amazon Unveils 'Haul'—Its Ultra-Discount Temu Rival Selling $1 Earrings and $8 Leggings*, FORTUNE (Nov. 13, 2024), https://fortune.com/2024/11/13/amazon-haul-temu-shein-discount-store-tiktok-shop/.

[81] Yunsieg P. Kim, *Micromanaging Technology*, 28 YALE J. L. & TECH. __ at 58 (2026).

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

Even though existing legal frameworks increasingly acknowledge the emergence of incognito consumer harms, they are ill-equipped to address such harms for two reasons. First, existing law assumes that someone will notice and report the harm, an assumption that incognito harm subverts by design. Both litigation and regulation rely on victims or observers detecting a problem and sounding the alarm, but invisible harms circumvent such triggers. Second, even when hidden harms do come to light, 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. As such, a system built for visible injuries falters in a world where injury is engineered to remain invisible.

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 tweaks to litigation procedure as the primary solutions to opaque, systemic consumer harms without explaining how those harms would be discovered in the first place, thus failing to resolve the detection gap between harms engineered to be invisible and an enforcement system that depends on someone noticing. Professor Andrew Miller, for instance, observes that algorithmic profiling can create "invisible" groups of disadvantaged consumers who might never realize that they were targeted.[82] Miller argues that litigation is crucial to uncovering "exploitation by powerful marketplace actors" and proposes refining procedural tools such as class actions and multidistrict litigation, to bring these hidden patterns to light.[83] Yet Miller highlights the catch-22 that his own argument represents, by relying on victims to sue even as he acknowledges that these consumers often do not know that they were harmed, leaving them unable to band together and sue.[84] Without any mechanism to trigger a case in the first place, his litigation strategy risks helping only the rare victim who notices the harm.

---

[82] *See* Miller, *supra* note 8, at 20.
[83] *Id*. at 50.
[84] *See id*. at 30 (discussing "the importance of making visible" groups harmed by algorithms).

Other works are afflicted by the same catch-22. Professor Nadiyah Humber urges a group-focused response to algorithmic housing discrimination by reviving the Fair Housing Act's "discriminatory effects" standard (especially segregative-effect theory) to challenge tenant-screening tools that perpetuate "algorithmic redlining."[85] This approach, if successful, would shift attention from individual denials to community-level outcomes.[86] But Humber's proposal does not fulfill the prerequisite: the bias must first become visible. She argues that more transparency would "allow declined tenants to seek redress,"[87] which implicitly concedes that many renters never realize they were algorithmically screened out. In short, Humber's solution of empowering affected groups to litigate via FHA doctrine presumes that someone actually discovers disparate impact. Without ex ante measures to surface hidden bias, even an expanded FHA theory would be left unused, reaching only the rare cases that happen to be discovered—such as when cases like *Louis v. SafeRent* expose the issue.[88]

Professors Peter Salib and Daniel Wilf-Townsend likewise place class action litigation at the heart of their answers to opaque algorithmic injuries. Salib argues that after *Wal-Mart v. Dukes*, many "high-merit, low-dollar" claims have little or no access to justice because they cannot meet class certification requirements under current doctrine.[89] *Wal-Mart* and its progeny disapproved of using statistics to establish commonality, effectively barring certain systemic bias cases from class actions.[90] The result, Salib argues, is that "untold numbers of meritorious claims . . . evaporate" absent an aggregation mechanism.[91] Salib's answer to this problem is procedural: 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 fail under existing law.[92]

Unfortunately, Salib's innovation would work only once the plaintiffs are already in court. It assumes that victims have discovered the hidden fee or

---

[85] Nadiyah J. Humber, *A Home for Digital Equity: Algorithmic Redlining and Property Technology*, 111 CAL. L. REV. 1421, 1469 (2023) ("illustrat[ing] the benefits of segregative effect theory and its potential application to algorithmic redlining").

[86] *See id*. at 1468 ("The burden-shifting approach gives both [plaintiffs and defendants] a more equal footing to claim and defend against unintentional discrimination.").

[87] *Id*. at 1430.

[88] *See id*. at 1424 (using *Louis v. SafeRent* to illustrate how "[l]andlords have long relied on imperfect proxies to turn down prospective tenants, [which] . . . very often track race.").

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

[90] *See id*. at 521-22 (*Wal-Mart v. Dukes* rejected "new, creative, and certification-facilitating methods of statistical proof" and made certification for "whole categories of putative class actions in a range of important doctrinal areas" including "consumer fraud").

[91] *Id*. at 521.

[92] *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").

algorithmic wrongdoing, organized, and sued. It does not address the trigger problem: who uncovers the incognito harm in the first place? Even a perfectly functioning AI jury, which is far from certain in the present day given AI's propensity for egregious errors at even basic tasks like cite-checking,[93] cannot deliver compensation or deterrence if the victims never realize that they were wronged. Thus, Salib's "AI jury" proposal merely underscores the gap between remedying harm and detecting it. Technology *may* someday streamline the former, but the latter still requires a catalyst outside the litigation process.

Wilf-Townsend does identify the detection paradox but still lands on a litigation-centric solution that falls short. He argues that "AI tools can create harms that are only demonstrable at the level of an affected group" which would "frustrate traditional individual claims" because biased lending, discriminatory ad targeting, and similar wrongs can be statistically invisible in any one instance and emerge only in large-scale patterns.[94] He contends that aggregation is not just an enforcement vehicle but 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.[95]

This proposal may lower the burden of remedy once a pattern is identified. Yet, like Salib's proposal, it implicitly presupposes that someone *will* detect the pattern. Wilf-Townsend does note that algorithmic audits or reporting duties could help surface group-level harms that are invisible at the individual level.[96] 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 necessitate aggregate litigation, he too leaves open the core question unanswered: how, absent proactive oversight, will the facts needed to plead such class action claims will ever come to light?

What emerges from these works is a consensus coupled with a dilemma. Scholars across the board agree that traditional individual litigation is ill-suited for the age of invisible algorithms and respond with structural solutions such as tweaking procedural rules and creating new theories of liability. These scholars propose the litigation-centric solutions that they do because they recognize that

---

[93] *See, e.g.*, Mike Scarcella, *Two US Judges Withdraw Rulings After Attorneys Question Accuracy*, REUTERS (July 30, 2025) ("research produced using artificial intelligence was included in a draft decision"), https://www.reuters.com/legal/government/two-us-judges-withdraw-rulings-after-attorneys-question-accuracy-2025-07-29/.

[94] Daniel Wilf-Townsend, *Artificial Intelligence and Aggregate Litigation*, 103 WASH. U. L. REV. __ (2026).

[95] *Id*. at 5, 41.

[96] *Id*. at 47.

unseen harms stay unremedied until they are first surfaced and then aggregated. Yet, their proposals still require someone to first notice and surface the harm. The detection gap thus remains the thorniest part of the equation, essentially the prerequisite to any of these reforms having purchase. The lesson, therefore, is that legal innovation must extend to mechanisms for *finding* incognito harms, not just for redressing them. Otherwise, even the most sophisticated class action or regulatory regime would be a strong engine idling without fuel, all dressed up with nowhere to go. Until the law devises better triggers for hidden harms, proposals like Humber's, Salib's, and Wilf-Townsend's, for all their merits, risk addressing only the tip of an unseen iceberg. They remind us that a legal system predicated on "notice" of harm will falter when no one is able to notice.

2. Spoliation Doctrine Is a Dead End

One might respond to the foregoing that litigation already has an answer to parties destroying unfavorable evidence—spoliation—and that it can address incognito consumer harm. But spoliation is as much a dead end here as aggregate litigation. Spoliation only activates once litigation is pending or reasonably on the horizon.[97] If evidence disappears *before* anyone anticipates a claim, spoliation rules offer no relief.[98] Common law and the Federal Rules of Civil Procedure shield parties from sanctions for data lost through routine operations prior to a reasonable anticipation of litigation.[99] In short, a wrongdoer who prevents victims from suing by keeping them in the dark until after the proof is gone circumvents spoliation sanctions, while achieving the same result as classic spoliation: the destruction of evidence of wrongdoing. The wrongdoer may achieve even *more* than classic spoliation if the victim never notices harm, as incognito consumer harm aims to do, since there would not even be a lawsuit.

Worse, technology increasingly ensures that no claim is "reasonably anticipated," often by exploiting fine print and dark patterns. Companies can quietly revise terms or privacy policies to authorize harmful conduct while providing little effective notice. In mid-2024, for example, Meta updated its

---

[97] *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.").

[98] *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].").

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

privacy terms to permit using personal data, including private photos that users never uploaded, to train AI models.[100] Users could technically opt out, but Meta buried the opt-out in settings, framed in vague and misleading language, and open only for a short time.[101] 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"[102]—a euphemism bearing no resemblance to what Meta actually does. The result is a preservation trap. By keeping most users unaware, and by structuring "consent" so any later paper trail favors the company, firms can ensure that no outcry or lawsuit arises in time for a duty to preserve evidence to attach. In that sense, the incognito strategy succeeds by preventing the very conditions that would trigger spoliation doctrine.

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—yet courts often treat an unrejected email as effective notice and spam messages are not returned as undeliverable.[103] The result is technical compliance with practical invisibility: consumers never see critical terms like arbitration clauses or settlement notices, and major providers auto-delete spam after 30 days,[104] erasing victims' opportunity to learn of their rights. This tactic was reportedly used by 23andMe after its data breach in 2023, as it mass-emailed customers about a new mandatory arbitration clause and gave only 30 days to opt out.[105] If the email landed in spam, as designed to happen for many,[106] victims could miss the window and unknowingly forfeit their right to sue over the breach. 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 if the law never even realizes that wrongdoing existed to begin with.

Unfortunately, neither scholars nor courts have addressed this problem. For decades, debates over spoliation focused on how often evidence destruction occurs and on whether spoliation should give rise to an independent tort claim or merely a sanction, not on the doctrine's inherent inability to remedy incognito

---

[100] *See* Oestreicher, *supra* note 10.

[101] *See id*. (the opt-out window in the European Union ended on May 27, 2025).

[102] *Id*.

[103] *See* Kim, *supra* note 61 at 613-35.

[104] *Id*. at 616 n.51.

[105] Pranav Dixit, *23andMe Frantically Changed Its Terms of Service to Prevent Hacked Customers from Suing*, ENGADGET (Dec. 8, 2023), https://www.engadget.com/23andme-frantically-changed-its-terms-of-service-to-prevent-hacked-customers-from-suing-152434306.html.

[106] *See* Kim, *supra* note 61 at 613-35.

harms. Empirical studies in the 1980s found that half of large-firm litigators surveyed deemed "unfair and inadequate" evidence disclosure a "regular or frequent" problem and 69% of surveyed antitrust attorneys reported unethical practices, with one of the most-cited abuses being the destruction of evidence.[107] In the 1990s, commentators warned that spoliation had become "an effective . . . and . . . growing litigation practice" threatening to undermine the integrity of the trial process.[108] By the early 2000s, many scholars were urging for the recognition of a standalone spoliation cause of action, reflecting a consensus that existing sanctions were inadequate deterrents.[109] Courts, however, have been skeptical.[110] 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 existing remedies were "generally effective" deterrents.[111] This argument 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—reasonable anticipation of litigation—is deliberately never reached, rendering spoliation doctrine a dead end for incognito harm.

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"[112] and "has repeatedly stated that it will consider complaints as a basis for deciding who to examine and/or investigate."[113] State attorneys general, too, rely on public complaints, "which often serve[] as the starting point for later enforcement actions."[114]

---

[107] Deborah L. Rhode, *Ethical Perspectives on Legal Practice*, 37 STAN. L. REV. 589, 598-99 (1985).

[108] Charles R. Nesson, *Incentives to Spoliate Evidence in Civil Litigation: The Need for Vigorous Judicial Action*, 13 CARDOZO L. REV. 793, 793 (1991).

[109] Chris W. Sanchirico, *Evidence Tampering*, 53 DUKE L.J. 1215, 1280 (2004) (the "general position among scholars [is] that [spoliation of evidence tort claims] should be maintainable").

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

[111] Cedars-Sinai Med. Ctr. v. Superior Ct., 954 P.2d 511, 520 (Cal. 1998); *see also*

[112] Angela Littwin, *Why Process Complaints? Then and Now*, 87 TEMPLE L. REV. 895 (2015).

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

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

While consumer reports are an indispensable component of enforcement, the flaw is evident: when harm is designed to be 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."[115] Enforcement rests with the Attorney General, who can act on a "reason to believe" a violation occurred, including consumer tips. On the eve of the law's effective date, the AG even urged New Yorkers to report retailers that fail to show the notice.[116] But this model assumes that consumers will notice a missing or faulty disclosure and report it. If firms quietly omit the sign, few, if any, citizens will know that a violation occurred.[117] A transparency mandate cannot deter hidden pricing discrimination when violators can plausibly bet that almost no one will detect the missing notice. In short, enforcement driven solely or even primarily by consumers reporting leaves regulators flying blind, which is precisely what incognito harm exploits.

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,[118] 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.[119] If an employer relies solely

---

[115] N.Y. Gen. Bus. Law § 349-a, at 2.

[116] *See Attorney General James Warns New Yorkers About Algorithmic Pricing as New Law Takes Effect*, OFFICE OF THE N.Y. STATE ATTORNEY GENERAL (Nov. 5, 2025) ("Attorney General James is encouraging consumers to file complaints . . . if they encounter algorithmic pricing that is not properly disclosed"), https://ag.ny.gov/press-release/2025/attorney-general-james-warns-new-yorkers-about-algorithmic-pricing-new-law-takes.

[117] Talia B. Gillis, *"Price Discrimination" Discrimination*, 15 HARV. BUS. L. REV. 99 (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.").

[118] 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 n.107 (citing Illinois' 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. 818, 836 (arguing that Illinois' Artificial Intelligence Video Interview Act is a "good template for other . . . states").

[119] 820 Ill. Comp. Stat. 42/5.

on AI with no human reviewer, the Act also requires an annual bias audit, collecting and reporting demographic data on hires and rejections to test for disparate impact.[120] Similarly, Maryland enacted a law requiring employers to obtain applicants' written consent before using facial recognition technology in job interviews.[121] In theory, these disclosure and self-reporting obligations should expose AI bias and protect job applicants from hidden discrimination.

In practice, these regimes would likely be just as ineffective at deterring hidden harms. The Illinois law's stringent audit requirement can be evaded by inserting a token human reviewer into the hiring process so that the AI tool is never officially acting "solely" on its own. 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 will 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. Thus, a disclosure-based law which assumes that transparency without oversight can cure algorithmic harms would end up with neither transparency nor cure.

Although scholars and legislators have proposed regulatory reforms to address technology-assisted harms that victims often cannot see, many such proposals still assume that someone will detect and report violations. 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.[122] In other words, Lemley envisions regulators acting even when consumers are unaware of the misuse of their data or the fine print stripping away their rights. But his proposal still assumes that regulators find out about the abuses in the first place. 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. Lemley argues persuasively that notice-and-consent in the consumer economy has become fictitious, and his suggestion that the FTC reinterpret its existing remit to fight consumer abuse[123] as opposed to waiting for unlikely new legislation is pragmatic. But whatever tougher standards that the FTC may settle on would still operate only after wrongdoing is discovered. Without mechanisms to uncover hidden violations, even an emboldened FTC would be a watchman waiting for an alarm that never sounds.

---

[120] 820 Ill. Comp. Stat. 42/20.

[121] Md. Code Ann., Lab. & Empl. § 3-717.

[122] Lemley, *supra* note 7 at 248.

[123] *Id*. at 258-59 (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").

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 be treated as stewards legally required to put users' interests first, thus owing a fiduciary duty to "refrain from self-dealing."[124] They urge legal standards that prohibit designs which "unreasonably exploit our cognitive limitations, biases, and predictable errors"—i.e., deceptive dark patterns.[125] They would also forbid undisclosed, user-harming data extraction undertaken for the company's own benefit. 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.[126] 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 can require that "at least 80 percent of consumers who are paying a given fee know the existence and amount of the fee" when they incur the fee.[127] Regulators would randomly survey customers to test their understanding and penalize the relevant company if the threshold is unmet.[128]

As compelling as it may sound in theory, the proposed duty of loyalty and the "performance-based" consumer protection rules would, in practice, share the weak point of Lemley's proposal and the AI regulations covered above: enforcement still relies on discovering a violation. While Richards and Hartzog argue that a breach of this fiduciary duty "would be a per se legal injury" that satisfies the harm requirement for legal action,[129] they propose no mechanism to monitor a company's opaque decision-making. Thus, a design choice that quietly and illegally benefits the company at consumers' expense can violate the duty long before any outsider notices. As for performance-based standards, they work best for things that can be openly tested, such as whether consumers understand fee structures. But when a harmful practice is entirely hidden—such as a vacuum cleaner recording video without notice[130]—there is nothing to test, as consumers cannot "understand" what they do not know exists. A firm could satisfy every benchmark for disclosed practices while committing a separate, concealed abuse. Moreover, the approach depends on regulators or auditors collecting the right data, which presupposes that they know what metrics to monitor. It can measure known problems, but truly invisible and unforeseen harms will often fall outside any predefined performance metric.

---

[124] Richards & Hartzog, *supra* note 14 at 964.

[125] *Id*. at 1011.

[126] *See id*. at 1005 ("Informational capitalism demands your personal data and your attention. Consequently, companies do everything . . . to make you feel safe to expose yourself online.").

[127] Willis, *supra* note 42 at 1812.

[128] *Id*.

[129] Richards & Hartzog, *supra* note 14 at 1012.

[130] *See* Fell, *supra* note 1.

Proposed reform by legislators and regulators also neglect the detection gap. The Algorithmic Accountability Act, a bill proposed in 2025, would require companies to assess and report risks of certain automated decision systems before deployment.[131] For example, companies would be required to conduct a bias audit of a hiring algorithm and submit results to the FTC.[132] 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,[133] 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 catching discriminatory or unsafe systems early rather than after they have quietly harmed thousands of people. But they, too, ultimately turn on detection: reports matter only if someone reviews them and verifies accuracy, and pricing mandates would work only if violations are exposed and pursued.

In sum, the various existing proposals discussed herein represent a necessary evolution toward prevention, shifting the focus from after-the-fact remedies to before-the-fact precautions. They begin to align legal incentives with the reality that we must seek out harm rather than wait for it to self-report. Yet they still risk addressing only the harms that announce themselves, while missing the vast swath of incognito injuries that by design fly under the radar. The real challenge, therefore, is developing ways to expose the harms that no one is looking for, not just those that regulators already know to look for. Until the law devises alarm bells for deliberately hidden misconduct, even laudable reforms like impact assessments or performance standards will be incomplete.

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

Section A has described the detection gap, the law's inability to surface injuries engineered to remain hidden. But that is only half the problem. Despite the intentional concealment, incognito consumer harm sometimes does come to light, whether through a hack, a whistleblower, or sheer accident.[134] Even then, however, plaintiffs face an uphill battle convincing courts that a "real" injury occurred because modern doctrine remains wedded to a narrow, traditional notion of harm, often excluding the kinds of harm that hidden schemes inflict. Three hurdles in particular (constitutional standing, pleading standards, and class certification requirements) conspire to deny relief for incognito consumer harms.

---

[131] Algorithmic Accountability Act, S. 2164, 119th Cong. §§ 3(b)(1)(A) (2025).

[132] *See id*. at § 3(b)(1)(D).

[133] *See* 16 C.F.R. § 464.3 ("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.").

[134] *See* Kwai, *supra* note 3 (Tea data retention revealed by hack); MegaLag, *supra* note 30 (Honey's tracking of users revealed in part due to anonymous insider leaking source code).

Article III standing requires a plaintiff to show an "injury in fact"—an invasion of a legally protected interest that is "concrete, particularized, and actual or imminent."[135] For defamation torts, standing requires that the alleged defamatory statements be "published to a third party."[136] In *TransUnion LLC v. Ramirez*, a large credit reporting company had falsely flagged thousands of consumers as potential terrorists in their credit reports.[137] 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.[138] Even though the relevant statute created a private cause of action against any credit reporting company that fails to follow "reasonable procedures to assure maximum possible accuracy" without a publication requirement,[139] the Court reasoned that "an asserted *risk of future harm*" was insufficient to create injury and third-party publication was a "longstanding" common-law requirement.[140]

The third-party publication requirement means that, even if incognito consumer harms are eventually exposed, courts may still treat them as non-cognizable absent evidence of disclosure to others. Consider slight variations on real privacy harms. In 2023, the FTC sued the Amazon-owned firm Ring for storing "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."[141] The dating app Tea collected photo IDs and selfies for verification, promised to delete them, but retained them for years until a hack exposed the data.[142] Now assume that Ring and Tea retained the videos and IDs in secret but, to their knowledge, never shared them with third parties and were never hacked. Further imagine that whistleblowers in both companies come forward so that the victims are now aware of the harm they suffered. In these hypotheticals, there is a clear invasion of privacy, but not the third-party publication that *TransUnion* requires. At most, the conduct would be framed as a deceptive omission or misrepresentation actionable under § 5(a) of the FTC Act, which often carry only modest penalties absent additional harm.[143]

---

[135] TransUnion LLC v. Ramirez, 594 U.S. 413, 424 (2021).

[136] *Id*. at 432.

[137] *Id*. at 419-20.

[138] *Id*. at 433.

[139] 15 U.S.C. § 1681e(b) (accuracy requirement); 15 U.S.C. § 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"); *TransUnion*, 594 U.S. at 454 (Thomas, J., dissenting) ("This Court has relieved the legislature of its power to create and define rights.").

[140] *TransUnion*, 594 U.S. at 432, 435.

[141] Complaint at 17, 19, Fed. Trade Comm'n v. Ring LLC [*Ring Case*], No. 1:23-cv-01549 (D.D.C. May 31, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/complaint_ring.pdf.

[142] *See* Kwai, *supra* note 3.

[143] *Cf.* Peter Ormerod, *Privacy Qui Tam*, 98 NOTRE DAME L. REV. 267, 270 (2022)

Scholars have criticized courts for "adopting a particular perspective on the nature and value of privacy" and for "shifting" standing law to "dismiss claims on the basis of their views on the nature and value of the asserted harms," which will "have effects far beyond the privacy cases that precipitated it."[144] But the problem is even worse than that critique suggests. It is not only that courts often treat privacy harms as cognizable only when information is shown to have been disclosed to third parties. It is also that victims, courts, and even the companies often do not know whether information was disclosed to third parties. This is because "hackers have an incentive to commit breaches without being detected" so they can continue breaching undetected,[145] a lesson familiar since at least World War II.[146] Incognito consumer harm is designed to exploit this uncertainty, by both hiding wrongdoing and obscuring whether the "publication" that modern standing doctrine requires actually happened. Yet, scholars focus on only the first half of the problem and not the second.

Setting standing rules aside, even when consumers suspect incognito harm, *Twombly* and *Iqbal* shape what counts as an "injury" in practice by requiring factual allegations that make a claim *plausible*, not just conceivable.[147] In modern privacy and technology disputes, that requirement too often tends to privilege injuries with externally legible footprints: disclosure to third parties, concrete downstream misuse, measurable financial loss, or other observable consequences. But incognito harm, by design, rarely presents those markers at the outset. The result is not simply that injured plaintiffs lack access to discovery. It is that the misconduct which is the most characteristic of incognito harm—undetected retention, undisclosed access, unobservable risk-shifting[148]—are reclassified as merely speculative or "conceivable" rather than cognizable.

Commentators have long noted the post-*Iqbal* catch-22: plaintiffs need discovery to obtain the facts that make a claim plausible, yet they cannot

---

("even successful [privacy enforcement] actions have extracted disappointing penalties and underwhelming concession."); Diane Bartz, *Amazon's Ring Used to Spy on Customers, FTC Says in Privacy Settlement*, REUTERS (June 1, 2023) (Amazon settled for $5.8 million in Ring case with FTC), https://www.reuters.com/legal/us-ftc-sues-amazoncoms-ring-2023-05-31/.

[144] 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).

[145] Yunsieg P. Kim, *Redefining "No Evidence of a Breach" in Election Security*, 76 SMU L. REV. F. 130, 137 (2023).

[146] *Id*. at 139.

[147] Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007); Ashcroft v. Iqbal, 556 U.S. 662 (2009).

[148] *See* Kwai, *supra* note 3 (Tea data retention revealed by hack); MegaLag, *supra* note 30 (Honey's tracking of users revealed in part due to anonymous insider leaking source code).

get discovery without pleading the facts plausibly.[149] Incognito harm intensifies that problem because concealment does double work. It withholds information *and* deprives plaintiffs of the very kinds of facts that courts routinely treat as the indicia of real-world injury. When information asymmetry is strategic (as in, when the product is designed so outsiders cannot observe how it operates) pleading doctrine becomes a substantive sorting mechanism. Injuries that leave no outward trace are treated as conjectural, while injuries that happen to surface look "real" enough to plead.[150] In that sense, plausibility doctrine can reward successful concealment by converting non-observability into non-cognizability.[151]

Proposals to ameliorate this issue without enabling so-called "fishing expeditions" often take the form of limited pre-suit or pre-dismissal discovery in asymmetric information cases.[152] Other works have argued that courts should credit "institutional" facts, such as agency investigations, public enforcement actions, technical audits, or other competent determinations, as a basis for plausibility where defendants control the relevant evidence.[153] For incognito consumer harm, the commonly applicable lesson is that pleading rules cannot be treated as a neutral screen. If legal cognizability is increasingly defined by what can be pled with outward-facing detail, then the injuries most likely to go unseen will predictably be the injuries that the law declines to recognize.

Finally, incognito consumer harm also collides with existing class action doctrine, which is ironically the procedural device most often invoked to address low-value, widespread consumer wrongdoing. Class actions are meant to make aggregate enforcement feasible where individual suits are not. After *TransUnion*, however, a damages class cannot meaningfully serve as a vehicle to remedy hidden injuries if many class members are deemed "uninjured" under Article III's narrow conception of cognizable harm. *TransUnion* held

---

[149] *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) (plausibility pleading "is a form of fact pleading by another name.").

[150] *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 (2021) (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).

[151] *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, 1238-42 (2021) (plausibility pleading "rewards the various concealment methods" used by conspirators, leading judges to dismiss claims that lack details that conspirators have successfully hidden).

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

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

that only class members who suffered a concrete injury may recover damages in federal court, and that "every class member must have Article III standing in order to recover individual damages."[154] That requirement is virtually a gift for incognito harm because concealment often ensures that many victims cannot show the kind of externally verifiable injury that existing doctrine requires, especially when injury is defined by third-party disclosure, realized monetary loss, or other public-facing manifestations.[155] The more a scheme succeeds at keeping the harm internal, ambiguous, or undisclosed, the more it produces a damages class that is either entirely uncertifiable or drastically underinclusive.

The Supreme Court has so far avoided clarifying when, exactly, the "every class member" requirement must be proven. *TransUnion* expressly reserved the question of whether each absent class member must demonstrate standing at the certification stage.[156] More recently, the Court granted review in Labcorp v. Davis to address whether Rule 23 permits damages classes with both injured and uninjured members, only to dismiss the case as improvidently granted and leave the question unresolved.[157] But the practical consequence of this doctrinal uncertainty is still predictable: defendants can leverage standing to fracture proposed classes, narrow definitions, and demand individualized showings that are hard to make when the injury's very existence and scope are the contested, concealed fact. This creates a paradox for incognito consumer harm. Class actions are often defended as the tool that can expose and deter systematic misconduct.[158] Yet modern standing doctrine makes class-wide relief hardest precisely where wrongdoing is the most successfully hidden—where many victims cannot prove dissemination, show individualized manifestations, or even know whether the doctrinal trigger for "concrete" injury occurred. In those cases, aggregate litigation does not solve the detection gap, but inherits it.

Taken together, standing, plausibility pleading, and class certification doctrine reveal a legal system that filters consumer harm through visibility, by treating injury as legally real only when it leaves an observable footprint. The visibility requirement predictably results in under-deterrence of incognito consumer harm because companies have incentives to migrate misconduct into forms that consumers cannot observe, cannot plead with specificity, and

---

[154] *TransUnion*, 594 U.S. at 431.

[155] *See supra* Part II, Section A, Subsection 1.

[156] *TransUnion*, 594 U.S. at 431 n.4.

[157] 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 . . . 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.").

[158] *See, e.g.*, Miller, *supra* note 8; Salib, *supra* note 89; Wilf-Townsend, *supra* note 94.

cannot aggregate into a certifiable class. A more realistic consumer protection regime must treat certain "invisible" injuries as injuries, rather than dismissing them as technical violations until some downstream disclosure or monetizable loss can be proven. Scholars critiquing *TransUnion* have argued that the Court's approach threatens to disable private enforcement of many modern privacy and consumer protection laws by insisting on the wrong harm analogues and the wrong evidentiary triggers for "concreteness."[159] However, in the incognito setting, the problem is worse. A standard that turns on demonstrable disclosure or individually legible loss does not merely narrow recovery, but also rewards concealment by turning non-detection itself into a liability shield.

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

Section C synthesizes the problems identified in Sections A and B—that the existing system does not detect incognito harms and, even when such harms are detected, the law struggles to recognize them as cognizable harms—into a single systemic dynamic. When detection is weak and injury is defined narrowly, the law develops a survivorship bias because it sees only the harms that surface and mistakes the visible subset for the full universe of consumer injury. The point is familiar from a famous lesson in statistics. 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" thought that the parts with the most bullet holes, the wings and fuselage, should be reinforced with armor.[160] But a young statistician named Abraham Wald saw the flaw in this logic: the data came only from the planes that survived. As Wald saw it, the parts that really needed to be armored were those where the surviving planes sustained the *least* amount of damage—the engine and cockpit—because the planes struck there apparently never made it back.[161] Survivorship bias is the mistake of reasoning from the cases that survive a filter while forgetting the unobserved cases that did not.

Incognito consumer harm exposes the same epistemic trap in law. The legal system's working picture of "consumer harm" is not drawn from a neutral census of injuries. It is drawn from the subset of injuries that become visible

---

[159] *See, e.g.*, Erwin Chemerinsky, *What's Standing After* Transunion LLC v. Ramirez, 96 N.Y.U. L. REV. ONLINE 269, 270 (2021) (*TransUnion* "places in doubt the ability to sue to enforce countless federal laws, ranging from the Freedom of Information Act to civil rights statutes, to environmental laws, to even the prohibitions of child labor in the Fair Labor Standards Act."); Solove & Citron, *supra* note 144, at (*TransUnion* "essentially nullified a key enforcement component of many privacy laws—private rights of action.").

[160] JORDAN ELLENBERG, HOW NOT TO BE WRONG: THE POWER OF MATHEMATICAL THINKING 13, 14 (2014).

[161] *Id*. at 13.

enough to trigger enforcement and then survive the system's screening rules. Section A described the first filter, detection. Much of consumer protection and enforcement is complaint-driven, whether the "complaint" is filed with an agency, brought to a lawyer, or even registered informally through app reviews and press coverage.[162] But a practice engineered to remain unobserved short-circuits those triggers, because victims do not complain when they do not know.

Section B described the second filter, legal cognizability. Even when a hidden practice is eventually exposed, modern doctrine often demands an outward-facing indication of injury before it treats the harm as real. Standing doctrine tends to treat concealed risk, loss of control, and informational deprivation as insufficient unless paired with something legible to outsiders, such as third-party disclosure or downstream misuse. Pleading doctrine then requires plaintiffs to allege the very facts that concealment withholds. And class action doctrine, especially after *TransUnion*, can narrow relief precisely where concealment makes individualized proof of "concrete" injury hardest.

Together, detection and cognizability create a structural survivorship bias. The harms that the law most often "sees" are those that (1) generated a signal strong enough to be noticed and (2) can be narrated in the forms that doctrine already recognizes. Courts form intuitions about what "real" injury looks like from the cases that reach them. Agencies infer what problems "exist" from the complaints they receive and the violations they can readily prove. Scholars build diagnoses from the record of litigated disputes and public enforcement actions. Each step is rational from the perspective of each player. The problem is that the record itself is a biased sample because incognito consumer harms are disproportionately filtered out before they ever become data.

This helps explain a recurring pattern observed in both litigation and regulatory scholarship. If one deals only with the visible subset of harms, the obvious strategy of the wrongdoers is to procedurally defeat colorable claims that victims have already brought or attempt to bring. Scholarship in this area is vibrant. Professor David Horton has written about how corporations avoid litigation by imposing contracts that mandate arbitration for "all disputes . . . in perpetuity."[163] Professor Maria Glover has examined how some corporate

---

[162] *See, e.g.*, Littwin, *supra* note 112 (CFPB "uses complaints to inform . . . enforcement actions"); Gersowitz, Libo & Korek, *Class Action Lawsuit Filed Against Ikea Over Dangerous Furniture* (last visited Mar. 5, 2025) (a law firm asking "[h]ave you or someone that you care about been injured by a[n] IKEA dresser,"), https://www.lawyertime.com/class-action-lawsuit-filed-against-ikea-over-dangerous-furniture/amp/; Claire Fahy, *Disney Backs Down From Effort to Use Disney+ Agreement to Block Lawsuit*, N.Y. TIMES (Aug. 20, 2024) (Disney dropped attempt to impose mandatory arbitration after unfavorable press coverage).

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

defendants have begun to revert to class actions following the "improbable" rise of mass arbitration, which featured thousands of individual claimants filing thousands of "*individual* arbitration demands" on corporate wrongdoers.[164] Professor Richard Frankel has studied how large companies have modified arbitration clauses to deter mass arbitration by, for example, imposing onerous pre-arbitration procedures that consumers must exhaust before filing arbitration claims.[165] Those tools are real and consequential, and reform efforts aimed at them are not mistaken. But for *incognito* consumer harm, these tactics are downstream of a far more decisive move: a firm that keeps its practice invisible can avoid not just liability, but also the very possibility of a claim. Invisibility functions as a pre-pleading, pre-standing, and pre-class-action liability shield.

Survivorship bias also distorts common assumptions about who is the most likely to commit consumer-facing wrongdoing. Conventional accounts often treat large, repeat-player companies as far more likely to commit consumer harm than small companies[166] because larger firms have the resources to conduct costly litigation[167] and the scale needed to reap large profits from misconduct.[168] This narrative correctly explains which firms are more or less likely to commit *conspicuous* harms, because victims of conspicuous harms are likely to bring claims and wrongdoers' sole refuge once a claim is brought is to resist liability through, for example, procedural means. But with *incognito* consumer harm, this narrative is unlikely to hold. Consider a stylized example. Assume that an incognito consumer harm is detectable by only one consumer in a thousand, and suppose only one consumer in a thousand who detects it brings a claim. A firm with a million customers would expect, on average, one complaint, while a firm with ten thousand customers can expect none. Holding per-customer gain from incognito consumer harm constant, the smaller firm's expected liability can be *lower* because it is less likely to be seen than the larger firm. The point

---

[164] J. Maria Glover, *Mass Arbitration*, 74 STAN. L. REV. 1283, 1288-89 (2022).

[165] 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 (2025).

[166] *Cf.* 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.").

[167] *See* Erin Ann 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, or disutility.").

[168] *Cf.* Dorothy S. Lund & Natasha Sarin, *Corporate Crime and Punishment: An Empirical Study*, 100 TEX. L. REV. 285, 341 (2022) ("for the largest firms, even sky-high penalties are likely viewed as just another cost of doing business.").

is not that large firms are innocent. It is that in a world of engineered invisibility, "repeat player" status is not the only, or even the best, predictor of who would commit harm. Incognito harm can be most attractive where the victim pool is small, fragmented, or transient, and where reputational feedback is weak.

This difference also affects the efficacy of the solutions to consumer harm. In standard economic terms, a punishment is as an effective deterrent to wrongdoing only to the extent that it is expected. For conspicuous, visible harms, the severity of punishment can be expected to be roughly proportional to the degree of deterrence because, at least in theory, punishment can be reasonably expected of anyone who commits harm. For incognito consumer harm, however, the expected cost of committing harm is affected both by (a) the severity of the punishment and (b) the likelihood of getting caught.[169] When detection probability collapses toward zero, even severe ex post remedies can become largely irrelevant in practice. The system may look strict on paper yet function as permissive in actual practice, because concealment drives the probability term down far faster than lawmakers can raise the sanction term.

Survivorship bias distorts our priors about not only the perpetrators, but also the type of consumer harm. The familiar kind is diffuse harm: small losses spread across many, which are rationally ignored by individual victims and therefore require aggregation in order to be litigated. A typical example is a hidden monthly fee of 61 cents that AT&T charged on millions of consumers and escalated up to $2 before a class action was brought.[170] But diffuse harm is only a visible subset of the broader universe of harm. AT&T likely started at 61 cents and escalated only to $2 to suppress the likelihood that anyone deems that fee to be worth the trouble of litigation. When the injury is not seen, however, that constraint relaxes. A firm can impose substantial per-capita injury—by extracting sensitive data, shifting risk, or silently degrading a product's quality—without provoking immediate resistance, precisely because consumers do not know what was taken from them. In that sense, incognito harm can undermine two stylized assumptions that often structure reform debates: that corporate wrongdoing will be (a) committed chiefly by large repeat players and (b) designed chiefly to be small and diffuse. Concealment changes both beliefs.

The survivorship bias problem is apparent in otherwise careful empirical scholarship on privacy and consumer harm. As this Article argues, firms are

---

[169] *See, e.g.*, Nuno Garoupa, *Optimal Magnitude and Probability of Fines*, 45 EUROPEAN ECON. REV. 1765, 1765 (2001) ("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.") (citing Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968)).

[170] Brodkin, *supra* note 35.

increasingly incentivized to harvest what consumers cannot see. Yet, the legal and scholarly record of "harms" disproportionately consists of the subset that becomes visible enough to litigate. Professor Charlotte Tschider's descriptive empirical study of data-breach litigation illustrates the selection effect. Tschider 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."[171] That framing is both precisely correct *and* shows why the dataset suffers from a survivorship bias. A study of *litigated* breach cases necessarily excludes breaches that were never detected, incidents detected but not meaningfully attributable, and injuries that courts refuse to treat as cognizable (or plausible) absent outward-facing indicia such as downstream misuse. The study can tell us a great deal about what courts do *once a breach becomes a claim.* It cannot, by design, see the larger universe of consumer privacy harms that never survive the detection and cognizability filters that define this Article's central problem.

For present purposes, the foregoing is less methodological criticism than a caution about inference and prescription. 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 treating the "typical" obstacle as the one courts confront *after* suit begins. But, as incognito consumer harm underscores, the front-end filters are often decisive: concealment suppresses complaints, counsel, cases, and suppresses the evidentiary preconditions for standing. A litigation-centered description of breaches, even when it candidly emphasizes standing as a barrier, can still crowd out the more basic question: how many privacy harms never reach court at all, and how much doctrinal "strictness" is simply an artifact of seeing only the rare cases that surface? Read in that light, Tschider's project is an instructive example of survivorship bias at work in the privacy literature. It reveals the contours of the visible subset while simultaneously reminding us how much remains systematically off-docket—and therefore off-theory—until detection-first mechanisms exist.

The point is not that the literature's existing tools are misguided in their own domains. Arbitration reform, class-action doctrine, and aggregation mechanisms are necessary responses to conspicuous, low-dollar wrongdoing. The point is that those solutions presuppose the very conditions that *incognito* harm is designed to defeat: detection and a legally recognizable account of injury. When the bottleneck is far upstream of a claim being filed, optimizing downstream adjudication can resemble armoring the wings of the planes that returned while neglecting the places where hits are least likely to be observed.

---

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

The implication for the remainder of this Article is straightforward. Sections A and B identified the system's twin failures, weak detection and narrow cognizability, while this Section explained why those failures are self-reinforcing. They shape the evidentiary record on which doctrine, enforcement priorities, and scholarly diagnosis rely. Hence, Part III turns from diagnosing doctrinal mismatch to designing detection-first institutions and information-forcing tools that can surface hidden practices ex ante and make concealed injuries actionable without waiting for an accident to supply missing evidence.

## 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 the system's front end. That is why many familiar reforms—tougher penalties, broader standing, looser certification—can matter at the margins but still miss the core pathology. They are downstream repairs to a system that fails upstream.

To be sure, some 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.[172] But such measures would still not address the structural problem at the core of incognito harms, because they presuppose that the concealment has already been punctured—by a hack, whistleblower, or accident. For a phenomenon defined by intentional invisibility, the legal system cannot treat discovery as an accidental prerequisite. Thus, meaningful reform must build discovery into the system's very design.

Part III therefore shifts the center of gravity from ex post remedies to ex ante revelation, in both litigation and regulation. The aim is not to abandon deterrence or compensation, but to recognize detection as a coequal pillar of consumer protection. When wrongdoers can profit by keeping conduct invisible, reforms that work only after a complaint is filed are structurally underinclusive. What is needed is a set of reforms that makes concealment harder to maintain, more likely to be discovered, and far more costly once it is eventually exposed.

---

[172] *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 (7th Cir. 2023) (distinguishing the case at bar from *Carlsen* without rejecting the benefit-of-the-bargain theory accepted by the 8th Circuit).

### *A. Beyond Tweaks: Embracing a Detection-First Paradigm*

A detection-first paradigm is not a radical invention. It is how the law already governs risks that are too catastrophic, too technical, or too opaque to leave to victim awareness. In high-risk sectors, regulators do not wait for harmed individuals to recognize wrongdoing and file a complaint. They routinely inspect, monitor, and audit, because the alternative is to learn about violations only after it is too late. Consider nuclear safety. The Nuclear Regulatory Commission's oversight model is inspection-heavy by design, including approximately 1,000 safety inspections annually across fuel, reactor, and materials licensees.[173] For operating plants, NRC specialists conduct routine inspections each year at each plant (often in the double digits), precisely because many safety risks do not self-report until after a safety failure.[174] The same logic animates environmental monitoring. Pollution harms are frequently invisible at the point of exposure, so environmental law often relies on mandated measurement and recordkeeping rather than consumer complaints. The EPA, for instance, requires continuous emission monitoring systems in certain contexts to enable ongoing compliance determinations and to catch violations that would otherwise stay undetected.[175]

Other familiar regimes follow the same template. The FDA conducts inspections to protect consumers from unsafe products,[176] and the FAA's safety oversight of airlines is explicitly organized around certification and surveillance rather than waiting for passengers to discover noncompliance mid-flight.[177] Banking supervision rests on the same logic: the Office of the Comptroller of the Currency describes examinations as fundamental to supervision and notes that full-scope, on-site reviews occur on a regular "supervisory cycle" (generally every 12-18 months).[178] These systems treat inspection and audit capacity as

---

[173] U.S. Nuclear Regul. Comm'n, *NRC at a Glance* (last visited Jan. 1, 2026) https://www.nrc.gov/about-nrc/nrcataglance.

[174] U.S. Nuclear Regul. Comm'n, *Backgrounder on Oversight of Nuclear Power Plants* (last visited Jan. 1, 2026) (describing routine inspections conducted each year at each nuclear power plant), https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/oversight.

[175] U.S. Env't Prot. Agency, *Continuous Emission Monitoring Systems* (last visited Jan. 1, 2026) (CEMS are required under some EPA regulations to enable continual compliance determinations or determination of exceedances), https://www.epa.gov/emc/emc-continuous-emission-monitoring-systems; 40 C.F.R. § 60.7 (recordkeeping and reporting requirements).

[176] U.S. Food & Drug Admin., *Types of FDA Inspections* (Sept. 13, 2024), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-basics/types-fda-inspections.

[177] Fed. Aviation Admin., *Air Carrier Oversight* (Mar. 31, 2022) (describing FAA's certification and surveillance responsibilities for air carriers), https://www.faa.gov/about/initiatives/sas/oversight.

[178] Bureau of Consumer Prot., Fed. Trade Comm'n (describing its role as stopping unfair and deceptive practices by "collecting reports from consumers"), https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection (last visited Jan. 1, 2026).

part of the legal infrastructure itself—not as an optional, after-the-fact response to public outcry. Political scientists have a vocabulary for this distinction. McCubbins and Schwartz distinguish "police patrol" oversight (monitoring by regulators) from "fire alarm" oversight (relying on third parties to report).[179]

The common thread among the examples of police patrol oversight cited above is institutional humility about victim awareness. These regimes assume that regulated entities will have informational advantages, that violations may be technically complex, and that harm may be widely distributed before any individual can perceive it. They therefore treat detection capacity—inspection authority, monitoring mandates, audit trails, and information flows—as an essential part of substantive protection. In contrast, consumer protection for privacy and digital products still leans heavily on a fire-alarm model: victims (or journalists, or even hackers) are expected to ring the bell. That posture can be rational when harms are legible and consumers can recognize and report them.

But incognito consumer harm exists precisely where the fire alarm is least likely to sound because misconduct is difficult to see from the outside—where firms can bury conduct in code, silence signals with obfuscation, and deprive victims of any reason to suspect wrongdoing. The consumer context is therefore anomalous in a way we have grown accustomed to ignoring. We regulate increasingly complex, ubiquitous, sensor-rich consumer products with a system that mostly lacks routine inspection capacity for those products' hidden behaviors. We have no consumer analogue of resident inspectors, mandatory black-box logging, or continuous compliance telemetry for the practices most likely to be incognito. The result is not merely under-enforcement. It is a predictable enforcement blind spot: an entire class of profitable misconduct that rational firms can expect to commit with low probability of detection.

Closing that gap requires a detection-first paradigm. That does not mean omnipresent surveillance of every app and device. It means rebuilding consumer protection around mechanisms that can generate reliable information about compliance even when no victim knows to complain. Recent scholarship on "regulatory monitoring" makes a similar fundamental point: modern markets increasingly require institutions that can observe business practices at scale rather than treating visibility as a natural feature of harm.[180] Put concretely, a

---

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

[180] *See, e.g.*, Van Loo, *supra* note 16 at 1631 (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

detection-first consumer protection regime would (1) allow, in carefully cabined ways, authorities (and even private parties) to seek out hidden harm without waiting for victim reports; (2) require verifiable audit trails for certain high-risk practices so that compliance is not purely self-attested; and (3) cultivate alternative information channels—whistleblowers, independent audits, technical testing, and risk-based inspections—to puncture secrecy where consumers cannot. Without this upstream reorientation, the law will remain structurally mismatched to incognito consumer harm: strong on paper, reactive in posture, and easy to evade by simply making sure that no "alarm bell" will ever ring.

### *B. Regulatory Reforms: Public Detection and Deterrence*

Because incognito consumer harm suppresses complaints, regulators cannot treat consumer reports as the default trigger for enforcement. A system that mostly waits for victims to notice harm is structurally mismatched to a phenomenon defined by engineered invisibility. Public enforcement therefore needs tools that (1) generate credible information about compliance even when no one complains and (2) make concealment an aggravating factor rather than a liability shield. Three reforms—targeted transparency rights that function as low-level audits, auditability-by-design through logging and telemetry, and stronger audit/whistleblower infrastructure—would move consumer protection from "fire alarm" to "police patrol" without requiring omnipresent surveillance.

#### 1. Data Transparency Rights With Teeth

A familiar starting point is the "right to know": the right to ask a firm what data it has, how it used them, and whether it deleted them.[181] Modern privacy law already contains versions of these rights. The California Consumer Privacy Act gives consumers rights to know what personal information is held by certain data handlers and to have such personal information deleted.[182] The European Union's General Data Protection Regulation (GDPR) similarly gives consumers a right to obtain confirmation on whether personal data is being processed, access to the data, and certain metadata about the processing.[183] For example, a German non-profit invoked the GDPR to know what information Honey collected about users, and learned that Honey records nearly everything

---

agencies and regulated entities alike; implementation of programs that depend on making difficult causal connections between regulated activities and environmental harms.").

[181] Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 994 (2023) ("The right to information is a fundamental part of privacy protection. Most privacy laws provide for this right. . . . The right often requires disclosing information about the data gathered about people; how the data is used, transferred, and protected . . . .")

[182] Cal. Civ. Code §§ 1798.105, 1798.110, 1798.115, 1798.130.

[183] Regulation (EU) 2016/679 (General Data Protection Regulation), art. 15, 2016 O.J. (L 119) 1.

users do online: the fact that a user "viewed the details for his AliExpress order 3002876007952992 a total of 13 times, starting on February 17 at 7:43 PM, . . . started a dispute for this order on February 25 at 10:01 AM. . . . [and] went looking for an Airbnb in Berlin-Mitte on February 24 at 8:02 PM. . . . for . . . a hotel room for two adults for the period from March 04 to March 05."[184] These rights matter for reasons of dignity and autonomy. However, in the incognito consumer harm setting, the underappreciated value of these rights is institutional because they can be designed to produce signals about hidden malicious conduct.

Unfortunately, transparency rights on their own are a weak alarm bell. As Professor Margot Kaminski put it, "[r]ights of notice, access, correction, even opt out—people won't know they have these rights," and firms forced to operationalize those rights will tend to operationalize the "weakest versions."[185] Solove similarly argues that rights-based privacy governance often places too much burden on individuals and can devolve into perfunctory compliance rather than genuine constraint.[186] Incognito consumer harm exacerbates this problem even further. If wrongdoing is concealed, most (if not all) consumers will not know when to exercise rights, and firms can treat the rights process as another site for obfuscation. Indeed, in the case of the PayPal-owned browser extension Honey, concrete evidence of its malicious activity on users' computers was revealed only after Honey left its own source code exposed and an unnamed person sent the code to an independent journalist for analysis and disclosure.[187]

The implication is not that transparency rights are futile, but that they must be paired with rights with teeth, such as incentives and verifiability. The core move is to convert a consumer's inquiry from a largely symbolic request into a low-cost, legally consequential audit prompt. Legislatures can create a narrow "verification right" for high-risk practices: a right to demand a certified answer to specific questions that matter for incognito harm. A user could demand, for example, a sworn response backed by auditable records to: (1) whether the firm still possesses identity-verification documents it promised to delete; (2) whether the firm shared or granted access to a specified category of sensitive data; or (3) whether any automated system made decisions about the user using protected traits or proxies. The point is to design questions that test binary, checkable propositions for which a false answer itself is evidence of concealment. In practice, the response could be required to be signed or

---

[184] *See* DATAREQUESTS.ORG, *supra* note 2.

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

[186] *See* Solove, *supra* note 181 at 1002 ("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.").

[187] MegaLag, *supra* note 30.

digitally attested by a compliance officer, and to be 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,[188] liability would attach even if the consumer cannot prove downstream misuse of their own data (for example, third-party disclosure). The injury is the denial of verifiable truth in a context where concealment is the mechanism of harm.

As for the enforcement lever, it can be liquidated damages calibrated to concealment. 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.[189] A consumer-protection analogue could impose statutory damages for false or materially incomplete verification responses, with higher damages or civil penalties when evidence shows 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.

To avoid turning verification rights into generalized discovery against companies, the right can be tightly cabined. It can be limited to (i) specified high-risk domains (biometrics, precise location, intimate images, children's data, identity-verification documents), (ii) firms above a size threshold, or (iii) practices that are already regulated but hard to detect, such as data retention promises, access restrictions, and profiling constraints. This law can also borrow limiting principles already familiar in access-rights regimes, such as protections for third-party rights and trade secrets.[190] The point is not to force the public disclosure of proprietary code or to turn every consumer into a litigant. The point is to create a low-cost, high-leverage mechanism for puncturing secrecy in the subset of harm settings where secrecy is itself the compliance strategy.

Finally, "rights with teeth" work best when paired with a public backstop. Private requests in the schemes above would create leads. Regulators should be able to aggregate those leads, through portals designed for suspected false responses, and to demand corroborating records when patterns emerge. Such a measure, assuming effective implementation, would transform decentralized consumer inquiries into an early-warning system. This early warning system would not be a substitute for public oversight, but instead be a pipeline of actionable signals in a world where harm is designed to leave no evidence.

---

[188] As for how consumers or regulators would know whether a company lied, I propose telemetry, audits, and whistleblower incentives. *See infra* Subsections 2-3, Section B, Part III.

[189] 740 Ill. Comp. Stat. 14/20.

[190] *See, e.g.*, Cal. Civ. Code § 1798.145(c)(1) ("protected health information" exempt from CCPA); *General Data Protection Regulation*, art. 15(4) (trade secrets exemption).

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,[191] consumers may not even know what to ask until after a leak or breach reveals the practice. In this case, the regulatory problem is not merely informational asymmetry, but also the absence of 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.

Yet again, the basic 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 safety regulation, flight data and cockpit recorders have long been required to ensure objective post-incident information.[192] Consumer technology needs an analogue for certain high-risk practices. The EU AI Act illustrates the logic in the digital setting. It requires high-risk AI systems to support "automatic recording of events" over a system's lifetime and ties logging to traceability and post-market monitoring.[193] It also requires providers to keep those logs for a minimum period and, critically, to give competent authorities access to them upon a reasoned request, to the extent that the logs are under the provider's control.[194] The Digital Services Act similarly requires annual independent audits for large online platforms and search engines and obligates firms to cooperate with auditors by providing access to relevant data, premises, and answers to questions.[195] Other EU digital regimes likewise build in proactive monitoring capacity through defined investigative timeframes.[196] The common theme is to operationalize transparency. The law not only tells firms what not to do, but also requires the preconditions for verifying that they did not do it.

To be clear, a U.S. consumer-protection analogue should not copy these regimes wholesale. The Digital Markets Act, for example, has been criticized for effectively requiring regulators to obtain information that they cannot obtain and, even if such information could be obtained, would become immediately outdated.[197] The better approach is to combine proactive investigatory capacity

---

[191] *See* Fell, *supra* note 1; Oestreicher, *supra* note 10.

[192] *See* 14 C.F.R. § 121.343.

[193] Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts. 12, 21(2), 2024 O.J. (L 2024/1689) 1.

[194] *Id*.

[195] Regulation (EU) 2022/2065 (Digital Services Act), art. 37, 2022 O.J. (L 277) 1.

[196] Regulation (EU) 2022/1925 (Digital Markets Act), art. 17, 2022 O.J. (L 265) 1; Press Release, Eur. Comm'n, *Commission Opens Investigation into Potential Digital Markets Act Non-Compliance* (Nov. 12, 2025) (Commission aims to conclude investigation in 12 months).

[197] *See* Yunsieg P. Kim, *A Revolution Without A Cause: The Digital Markets Act and Neo-Brandeisian Antitrust*, 2023 WIS. L. REV. 1247, 1255-56 (2023).

with a clear, narrow set of required disclosures and a streamlined, low-cost process for obtaining them. Thus, the broader design principle carries: in certain domains where harm is easy to hide, compliance must be made inspectable. For certain practices, 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, intimate images); and (3) automated decision events for regulated uses (e.g., when an algorithmic system 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 point 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 underlying content.[198] Second, access must be controlled and confidential. Trade secret and privacy concerns are real, but they are solvable through mechanisms routinely used elsewhere: limited-purpose access, secure data rooms, protective orders, and sanctions for unauthorized disclosure.[199] The goal is emphatically not to let regulators read everyone's messages. Rather, it is to ensure that companies cannot evade accountability by designing systems with no built-in audit trail.

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."[200] In 2024, the FTC voted to use 6(b) compulsory process to study "surveillance pricing," focusing on intermediaries that market data- and AI-driven tools for individualized pricing.[201] The FTC

---

[198] *See, e.g.*, Ahmed I. Taloba & Alanazi Rayan, *A Privacy Preserving Medical Data Management Framework Using Blockchain Enabled Encrypted Role Based Access Control*, 15 SCIENTIFIC REPORTS 43864 (2025) ("[A]ll data is logged on the distributed ledger, thus being auditable and resistant to tampering. . . . Encrypted RBAC supports dynamic, role-based policy enforcement without disclosure of sensitive metadata").

[199] *See, e.g.*, Fed. Trade Comm'n v. Sysco Corp., 83 F. Supp. 3d 1, 5 (D.D.C. 2015) (granting a party's request to have data "made accessible . . . through a secure electronic data room or document review platform or document review platform"); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1353 (2018) ("courts may issue protective orders to limit the use and distribution of trade secrets beyond the needs of the proceeding").

[200] 15 U.S.C. § 46(b) (2018).

[201] Fed. Trade Comm'n, *6(b) Orders to File Special Report Regarding Surveillance Pricing Involving Intermediary Companies* (July 23, 2024).

has also published early staff perspectives on that 6(b) study.[202] Whatever one may think of the FTC's ultimate policy choices—and opinions are clearly divided[203]—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.

Crucially, 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. That is why, for discrete high-risk categories of consumer tech, Congress and states should require audit trails as a condition of operation. If a firm can profit by building systems that cannot be audited, it will. If the law makes auditability part of the compliance obligation, much like record-keeping obligations in other regulatory domains, it can change the engineering incentive: secrecy becomes costlier than simply obeying the law.

3. Proactive Audits and Whistleblower Incentives

Even with verification rights and telemetry, regulators will miss what they are not looking for. Incognito harm thrives on novelty: new intermediaries, new data uses, 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 resembles what 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."[204]

Start with audits. In many consumer domains, U.S. regulators lack the kind of routine examination authority that makes police-patrol oversight real.[205] But they can approximate it through a mix of (1) risk-based technical audits,

---

[202] Fed. Trade Comm'n, *Issue Spotlight: The Rise of Surveillance Pricing* (Jan. 17, 2025).

[203] *See, e.g.*, Zephyr Teachout, *The Long Future of the Neo-Brandeisian Movement, in Three Parts*, NETWORK L. REV. (Summer 2024) (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, *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.").

[204] ROBERT H. BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF 6 (1978).

[205] *Cf.* Willis, *supra* note 42 at 1397-98 (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* notes 112-14 and accompanying discussion (reliance of federal and state consumer protection law enforcement on consumer complaints).

(2) compulsory reporting targeted at high-risk practices, and (3) sustained investment in in-house technologists who can interpret what they find. The point is not to audit every app. It 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 surveillance.[206] Algorithmic impact-assessment literature makes the related point that audits and assessments are governance tools only to the extent that systems exist to evaluate them, enforce them, and learn from them over time.[207]

Next, incentivize third-party detection. Hidden corporate misconduct can be exposed by competing firms or independent researchers long before regulators ever suspect anything amiss.[208] 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.[209] Clarifying the liability landscape for responsible research would increase the odds that hidden abuses are uncovered by someone other than a hacker with malicious intent.

Finally, and most importantly, protect and reward insiders. Incognito consumer harm is frequently revealed not by victims but by people with access: engineers, compliance staff, contractors, and auditors. Recent scholarship on tech whistleblowing emphasizes that "radical information asymmetries" make

---

[206] *See, e.g.*, Gillis, *supra* note 117 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) ("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. JURISPRUDENCE REV. 345, 354 (2019) ("Manufacturers of IoT products have little interest in disclosing . . . just how much data manufacturers are collecting about consumers.").

[207] *See, e.g.*, Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J.L. & TECH. 117, 118 (2021) ("An AIA regulation has two main goals: (1) to require firms to consider social impacts early and work to mitigate them before development, and (2) to create documentation of decisions and testing that can support future policy-learning").

[208] *See, e.g.*, Myron Levin, *Rival's Tip Led EPA to Penalize Pesticide Firm in Chatsworth*, L.A. TIMES (June 13, 1985) (EPA penalty against a firm for illegal marketing "resulted from a tip from a rival distributor"); MegaLag, *supra* note 30 (independent journalist exposed Honey).

[209] *Department of Justice Announces New Policy for Charging Cases Under the Computer Fraud and Abuse Act*, DEPARTMENT OF JUSTICE (May 19, 2022), https://www.justice.gov/archives/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act.

internal disclosures a de facto source of governance information in the absence of "meaningful, rigorous, and systematic transparency rules."[210] In an incognito world, whistleblowing is not an optional accessory, but rather an indispensable infrastructure. The dearth of whistleblower provisions in consumer protection law[211] and, where such provisions exist, the dearth of monetary rewards for whistleblowers[212] are particularly quaint, given that whistleblower programs with money rewards are used in many other domains of the law. The SEC's whistleblower program authorizes awards of 10% to 30% of monetary sanctions collected in successful enforcement actions.[213] The False Claims Act similarly uses qui tam relators to expose fraud that the government would otherwise miss, rewarding successful relators with a share of recoveries.[214] These regimes recognize a premise that maps cleanly onto incognito consumer harm: when violations are hard to observe from outside, internal informants and motivated private enforcers are often the cheapest, most effective, and even only detectors.

Given the above, a detection-first consumer protection regime should strengthen (1) anti-retaliation protections; (2) confidential reporting channels to agencies with technical staff who can evaluate tips; and (3) 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, as in other regimes, from penalties recovered in successful actions.[215] To avoid perverse incentives, eligibility can be conditioned on responsible disclosure, preservation of evidence, and cooperation with investigators. The throughline across these reforms is simple. Public enforcement must stop treating detection as exogenous. It must treat detection capacity as a core design choice, something that the law can build. When the legal system makes concealment cheap, rational firms will conceal. When the legal system makes concealment risky and costly—by turning targeted questions into enforceable obligations, requiring auditability by design, and protecting those who can see inside the black box—incognito consumer harm would become much harder to sustain and far less profitable.

---

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

[211] 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 et seq., or the Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692 et seq.

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

[213] 15 U.S.C. § 78u-6(b)(1).

[214] 31 U.S.C. § 3730(d).

[215] *See, e.g.*, Benjamin J. McMichael, Mackenzi Barrett & W. Kip Viscusi, *A Constitutional False Claims Act*, 102 WASH. U. L. REV. 677 (2025) (discussing False Claims Act reward structure); Chinyere Ajanwachuku, Note, *An In-House Counsel's Decision to Whistleblow*, 25 GEO. J. LEGAL ETHICS 379, 380 (2012) (discussing SEC whistleblower reward structure).

### *C. Litigation Reforms: Unmasking Harm in Private Enforcement*

Even if public enforcement does become more detection-first, private litigation will remain a central tool against incognito consumer harm. Regulators will miss at least some violations for reasons no more sinister than the simple and inevitable fact that deterrence is not always perfect.[216] Private enforcement supplies a second channel for deterrence and compensation and, critically, a public airing of facts that perpetrators would prefer to keep buried. But incognito consumer harm is engineered to defeat the basic premises of ordinary civil litigation: that plaintiffs can discover enough facts to plead a claim, establish a cognizable injury, and aggregate low-value claims into a viable enforcement vehicle. The reforms below aim to make concealment backfire rather than pay, and to give plaintiffs a viable if narrow path to get the minimum information needed to litigate without turning every single case into open-ended discovery.

#### 1. Penalize Concealment-by-Design as Constructive Spoliation

As discussed above, classic spoliation doctrine is largely a dead end as a solution to incognito consumer harm because preservation duties typically attach only once litigation becomes pending or reasonably foreseeable.[217] That limitation creates a perverse incentive. If a perpetrator keeps victims unaware for long enough or designs systems to avoid leaving auditable traces, it can often avoid both liability and spoliation sanctions. Incognito consumer harm thus reveals an enforcement gap that spoliation doctrine was never designed to address: the deliberate prevention of lawsuits by preventing awareness, not merely the destruction of evidence after a claim is anticipated or already filed. A targeted solution is to treat intentional concealment that impairs proof as a spoliation analogue—call it *constructive spoliation*—and to attach litigation consequences once concealment is shown. The core idea is simple. When a defendant's design choices or communications are plausibly aimed at keeping a violation undiscoverable (or at ensuring that proof will not exist by the time that victims find out), courts should stop treating intentional invisibility as just another neutral fact and instead treat it as an aggravating wrong for litigation.

Operationally, courts could implement constructive spoliation through a small set of predictable, cabined tools. The first potential tool is evidentiary presumptions tied to concealment. If plaintiffs can make a threshold showing—through internal documents, whistleblower testimony, technical analysis, or

---

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

[217] *See supra* Part II, Section A, Subsection 2.

admissions in parallel proceedings—that a firm designed its product or notice architecture to prevent detection of a legal violation, courts should be willing to draw adverse inferences and presumptions that ordinarily require a preservation duty. The presumption need not decide the entire case, but it can be limited to the proposition most directly undermined by concealment. For example, if a company's system is built to auto-delete the access logs that would reveal unauthorized employee viewing of sensitive video,[218] the court could presume that unauthorized access did occur in the relevant period, leaving the defendant the burden to rebut with other evidence. Likewise, if a firm intentionally designs required "notice" not to be delivered by designing emails to go to spamboxes,[219] 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,"[220] and longstanding doctrine presumes that any destroyed evidence was adverse to the perpetrator.[221] 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 misses the point. Destroying evidence once litigation is pending and engineering concealment to ensure that litigation never begins both ensure the end result 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 potential tool is burden-shifting on the "unknown" facts that concealment makes unknowable. Incognito harm turns litigation into a contest over information gaps. Was personal information accessed? Was it shared? Was it retained past deletion promises? Did an algorithm use prohibited traits? When the 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 not radical. It is a familiar response when a party's own wrongful conduct prevents ordinary proof.[222] The key point is to require a meaningful threshold showing of intentional concealment, not mere complexity or ordinary confidentiality.

---

[218] *See Ring Case*, Complaint at 17, 19.

[219] *See* Kim, *supra* note 61 at 613-35.

[220] *See* Fed. R. Civ. P. 37(e); Silvestri v. Gen. Motors Corp., 271 F.3d 583, 590-94 (4th Cir. 2001) (affirming dismissal of lawsuit as sanctions after spoliation prejudiced adversary).

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

[222] *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) (abrogated on other grounds by the Portal-to-Portal Act of 1947, 29 U.S.C. §§ 251-262).

Recent consumer protection law literature has proposed responding to modern information asymmetry with burden shifting, but they still presuppose that a plaintiff (or regulator) can first surface 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.[223] 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 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 possible way 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 remains hidden until limitations periods, opt-out windows, or cancellation rights have lapsed. Courts already recognize doctrines like fraudulent concealment and equitable tolling in certain settings,[224] 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, then to argue it was discovered "too late."

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, 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

---

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

[224] *See, e.g.*, Holmberg v. Armbrecht, 327 U.S. 392 (1946) (equitable tolling recognized in federal law where fraud concealed the cause of action).

choices that delete compliance-relevant audit trails while preserving business-relevant data, deliberate use of obfuscatory notification language, or intentional routing of notices through channels likely to be missed. In other words, the trigger should be purposeful design or communications aimed at invisibility, 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.[225]

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

Incognito consumer harm collides with the plausibility pleading regime of *Twombly* and *Iqbal*[226]: the most probative facts are often exclusively held by the defendant, and plaintiffs can be dismissed before discovery begins. This is not only a pleading doctrine problem, but also an information-access problem. If the legal system wants private enforcement to function for hidden harms, it requires a narrow mechanism for plaintiffs to obtain the minimum facts necessary to plead and litigate without authorizing fishing expeditions.

A workable model is cabined pre-suit or early-stage discovery—not full discovery, but targeted information-forcing on specific, checkable questions. U.S. law has building blocks, but they are underpowered for incognito harm. Federal Rule of Civil Procedure 27, for example, allows pre-suit depositions to perpetuate testimony, not to investigate whether wrongdoing occurred.[227] Several states go further. Texas's Rule 202 is a well-known example of a procedure permitting pre-suit depositions to investigate potential claims, subject to limitations and balancing.[228] Recent civil procedure scholarship likewise argues that limited pre-suit discovery can reduce loss of electronically stored information and the asymmetry that obstructs otherwise colorable claims.[229]

In the incognito harm context, a calibrated procedure could look like the following. The first step is a heightened threshold showing. A plaintiff would need to present a specific, credible basis for suspicion, such as a whistleblower

---

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

[226] *Twombly*, 550 U.S. at 544; *Iqbal*, 556 U.S. at 662.

[227] Fed. R. Civ. P. 27(a)-(c).

[228] *See* Tex. R. Civ. Pro. 202.1 ("A person may petition the court for an order authorizing the taking of a deposition on . . . either . . . for use in an anticipated suit; or . . . a potential suit"); In re Jorden, 249 S.W.3d 416, 422 (Tex. 2008) (accrual and unknown essential facts in the Rule 202 context); In re Doe, 444 S.W.3d 603, 610-12 (Tex. 2014) (Rule 202's scope and limits).

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

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 just a hunch, but can be weaker than the full proof that current pleading doctrine effectively demands.[230] The second step is narrow, question-driven discovery. Courts could authorize only what is necessary to answer a small set of binary 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.

The procedures described above 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 the litigation.[231] 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.[232] In the incognito context, those materials are not opportunistic shortcuts; they are often the only realistically available answer to a fatal information asymmetry.

---

[230] *See* Miller, *supra* note 149.

[231] *See* Fed. R. Civ. P. 26(c) (protective orders); id. 26(b)(1) (proportionality).

[232] *See, e.g.*, Marcus Alexander Gadson, *Stolen Plausibility*, 110 GEO. L.J. 291, 324 (2021) (discussing courts "sanctioning plaintiffs for borrowing plausibility").

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 analogues can convert hidden invasions into "no injury" unless third-party disclosure or downstream misuse is shown.[233] 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 to this problem 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 *alone* would not solve standing after *TransUnion*, but they would do two important things. First, they make harms redressable without individualized proof of monetary loss. Second, they 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.[234] A federal or state analogue could target the incognito core: undisclosed retention past 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 shift 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 crucial 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)[235] 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

[233] *See supra* notes 135-147 and accompanying discussion.
[234] 740 Ill. Comp. Stat. 14/20 (2024).
[235] *See supra* Part III, Section B, Subsection 1.

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."[236]

Recent privacy-law scholarship focused on 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 a federal privacy regime is designed with litigation realities in mind.[237] Incognito consumer harm strengthens that argument. If legislatures want private enforcement, they cannot write liability rules that presuppose visibility and then leave courts to apply standing doctrine that demands visible manifestations of invisible harm.

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) standing fights over uninjured members that can defeat certification or narrow down class definitions. As noted in the discussion on the current law's failure to recognize certain incognito consumer harms as injuries, *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.[238] The Court's later decision to dismiss *Labcorp v. Davis* as improvidently granted preserved the circuit split and the practical uncertainty intact.[239] A recent CRS analysis also framed the post-*TransUnion* question as a live and consequential design problem for aggregate litigation.[240]

---

[236] *Senator Josh Hawley, Sen. Blumenthal Unveil Bipartisan Bill Empowering Working Americans to Sue Big Tech, AI Companies for Stealing Creative Works*, JOSH HAWLEY, U.S. SENATOR FOR MISSOURI (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/; S. ___, 119th Cong. § 3(b)(1) (1st Sess. 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.").

[237] *See, e.g.*, Nabil Shaikh, Comment, *Surveillance Class Actions: Reconstructing a Federal Data Privacy Private Right of Action*, 172 U. PA. L. REV. 865, 867-68 (2024) ("several procedural requirements, including Federal Rule of Civil Procedure 23 and Article III standing, often doom surveillance class actions . . . . [The author] makes several substantive recommendations for a federal privacy law that can give effect to a private right of action.").

[238] *TransUnion*, 594 U.S. at 431 n.4.

[239] *Lab'y Corp.*, 605 U.S. at 327; *id*. at 328 (Kavanaugh, J., dissenting).

[240] Bryan L. Adkins, *Supreme Court Considers Whether Federal Courts May Certify*

Incognito harm suggests several aggregation reforms that do not require courts to award damages to truly uninjured people, but that also do not let stealth immunize wrongdoing. One is issue certification and staged adjudication. Courts can certify common liability issues under Rule 23(c)(4) and reserve individualized injury/damages questions for a later phase or claims process. This is not a silver bullet, but it can reduce the defendant's leverage to turn "some members might be uninjured" into total defeat of certification in cases where the core conduct is uniform and primary disputes are common. Another possible reform is injunctive and declaratory class relief where appropriate. When the goal is to stop ongoing hidden practices—retention, access, covert collection—injunctive relief can be more meaningful than damages. Properly structured Rule 23(b)(2) classes can sometimes avoid the most paralyzing individualized standing disputes at the certification stage, while still requiring standing for the named plaintiffs and ensuring that relief is properly targeted.

A third 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 litigation,[241] 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. Finally, litigants can exploit fraud-and-deception framing where it fits. Some incognito harms can be litigated when reframed as 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 doctrines. The point is not to force every case into fraud. It is to recognize that courts already understand deception injuries better than "data handling" injuries, and litigants can exploit that doctrinal reality once concealment is punctured.

---

*Class Actions When Some Proposed Class Members Are Uninjured*, CRS LEGAL SIDEBAR LSB11317 (May 27, 2025), https://www.congress.gov/crs-product/LSB11317.

[241] *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, 442 (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").

Taken together, these litigation reforms share a single aim: to make concealment an ex ante liability risk rather than an ex post liability shield. Public detection-first reforms can increase the rate at which hidden harms are found. But unless private enforcement can then translate discovery into viable claims—via concealment-sensitive evidentiary rules, narrow early discovery, legislatively recognized injuries, and workable aggregation rules—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 discussed in Part III thus far can be organized along two cross-cutting axes: minor vs. structural reforms, and litigation vs. regulation as the primary enforcement channel. Those axes may seem to represent binary choices, but they are not. The core claim of this Article is instead architectural. Because incognito consumer harm is defined by engineered invisibility, the system's front-end detection tools must be rebuilt, and only then can the familiar back-end tools of liability, damages, and aggregation do meaningful work.

Consider the first axis, minor versus structural change. Minor reforms—creative pleading (like benefit-of-the-bargain deception), doctrinal refinement of tolling, incremental procedural flexibility, and targeted statutory damages—can matter at the margins *once misconduct is exposed*. They can also reduce the extent to which courts dismiss concealed practices as "no harm" merely because the injury is hard to monetize or narrate in common-law analogies. But incognito consumer harm is the setting where marginal changes are most likely to be ineffective, because the bottleneck is often upstream of the merits. Deterrence turns not on what the law says will happen *if* a violator is caught but on the expected sanction, which depends on both the sanction's severity and the probability of detection.[242] When that probability approaches zero, raising penalties, expanding standing, or loosening certification can produce a system that seems strict only on paper.[243] Structural reforms—whistleblower rewards, auditability-by-design, risk-based inspections, and verification rights that create legally meaningful answers—depend on that missing probability term. Structural reforms may be costly, but they are the difference between a regime that waits for an accident and one that can routinely find what it is not supposed to see.

This logic explains why litigation and regulation should be treated as complements rather than substitutes. U.S. law already relies heavily on private

---

[242] *See* Becker, *supra* note 169 and accompanying discussion.

[243] A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LIT. 45, 47 (2000) (one will commit a wrong "taking into account . . . the chance of his being caught and sanctioned); *id*. at 47-55 (modeling offender behavior).

enforcement to implement public policy, including in the consumer economy.[244] But private litigation is structurally deficient in the incognito setting for the reasons Part II described. Plaintiffs cannot plead what they cannot observe. Courts often demand outward-facing indicia of injury. Aggregation doctrine is easiest to weaponize when many class members cannot prove the very facts concealment obscures. That does not mean that litigation is useless, but it means that litigation needs upstream inputs that it cannot reliably generate on its own. Regulation, properly designed, can supply those inputs by creating verifiable information flows such as audit trails, mandated logging, and protected reporting channels that translate hidden design choices into actionable, concrete records.

Conversely, litigation can provide benefits that regulation routinely undersupplies. Even well-resourced agencies cannot patrol everything,[245] and agencies often lack the incentives, remit, or resources to pursue every category of abuse that private litigants can pursue once the facts are known.[246] Litigation can produce public factual records through discovery, expert testimony, and adjudication, compensation or disgorgement that returns value to victims, and reputational consequences that are difficult for agencies to replicate through civil penalties alone.[247] In that sense, private suits function as a kind of "fire alarm" channel—an enforcement sensor outside the state—while structural regulatory monitoring functions as the "police patrol."[248] The point is not that one is superior, but to avoid building a consumer-protection system that relies on fire alarms in the very area where wrongdoers profit by disabling the alarm.

This complementarity also shows how tradeoffs and sequencing can be pursued. Some tools of structural reform suggested above such as telemetry,

---

[244] *See* David L. Noll & Luke P. Norris, *Federal Rules of Private Enforcement*, 108 CORNELL L. REV. 1639, 1641 (2023) ("State and federal legislatures, at times helped by courts, have deliberately encouraged private enforcement [with] . . . measures that make it attractive for private parties and the attorneys who represent them to shoulder the work of enforcing the law").

[245] Raskolnikov, *supra* note 216 at 1157 (even "the optimal regulation" must assume that "irredeemable acts . . . cannot be perfectly deterred.").

[246] *See, e.g.*, Z. Payvand Ahdout, *Enforcement Lawmaking and Judicial Review*, 135 HARV. L. REV. 937, 975 (2022) ("The Executive is constrained by resources and politics from enforcing all laws against all people and entities."); Margaret H. Lemos & Max Minzner, For-Profit Public Enforcement, 127 HARV. L. REV. 853, 859 (2014) ("public enforcers, because they are paid by salary, have no direct financial stake in the success of litigation.").

[247] *See, e.g.*, Roy Shapira, *A Reputational Theory of Corporate Law*, 26 STAN. L. & POL'Y REV. 1, 11 (2015) ("[Aside from legislation and regulations, litigation . . . can draw market players' attention to previously unnoticed corporate misbehavior. . . . The mere filing of a lawsuit (not to mention information revealed during litigation) may attract the attention of other stakeholders and propel them to downgrade their beliefs about the company.").

[248] *See* McCubbins & Schwartz, *supra* note 179 at 166 (describing distinction between police-patrol oversight and fire-alarm oversight).

logging, audits can seem intrusive in the abstract and, depending on how they are implemented, can become unduly intrusive in practice. A recent example is Google automatically tracking user activity for child sexual abuse material. While well-intended, it sparked backlash when it led to false positives. In one case, a user sent photos of his "son's groin to send to a doctor after realizing it was inflamed" so a doctor could "prescribe antibiotics."[249] Google flagged the photos as CSAM and a police investigation was opened against the user. [250]

But, as briefly discussed, telemetry can be designed to be narrow and protective through safeguards such as data minimization, confidentiality, risk-based triggers, and independent auditing rather than unlimited access.[251] At the same time, some "minor" litigation reforms become more defensible once structural reforms exist. For example, early, question-driven discovery is less likely to devolve into open-ended fishing if there are already mandated records and audit trails that can answer a small number of binary questions quickly.[252] Likewise, concealment-sensitive presumptions and burdens are easier to confine when the trigger is not merely "complexity" but concrete evidence of deliberate efforts to defeat detectability, which is precisely the evidence that monitoring, whistleblowers, and auditability obligations are designed to easily produce.

To synthesize, then, the choice is not to regulate *or* litigate, nor to tweak *or* rebuild. The truly optimal choice is a coordinated package that (1) raises the probability of discovery for hidden practices, (2) preserves the ability to translate discovery into liability through cabined procedural and substantive adjustments, and (3) treats concealment as an aggravating factor, not a liability shield. A responsive enforcement scheme encompassing information-forcing, auditing, penalties, and private redress when concealment is detected fits such a setting better than a system that tries to do everything with ex post damages alone. The objective is to flip the playbook, by turning invisibility from what makes misconduct profitable to what makes misconduct risky and highly costly.

## CONCLUSION

Incognito consumer harm is not just another category of consumer injury. It is an enforcement strategy to design wrongdoing so that most victims

---

[249] Johana Bhuiyan, *Google Refuses to Reinstate Man's Account After He Took Medical Images of Son's Groin*, THE GUARDIAN (Aug. 23, 2022), https://www.theguardian.com/technology/2022/aug/22/google-csam-account-blocked.

[250] *Id*.

[251] *See supra* note 199 and accompanying discussion.

[252] *See supra* Part III, Section C, Subsection 3.

never realize that anything happened, and the law's usual triggers of litigation, investigations, and regulation never activate. When illegality is engineered to be unobservable, a system that depends on victims noticing will predictably under-enforce, and doctrines that demand outward-facing proof of "real" injury will predictably reward the most successful concealment. The result is not merely uncompensated victims, but a deeper corrosion of market legitimacy. Consent becomes increasingly fictional, and the public record of consumer harm becomes a biased sample drawn from the rare cases that surface by accident.

The central prescription of this Article is thus architectural. Consumer protection must treat detection capacity as part of the legal design, not as an external contingency. The practical goal is simple: make concealment risky and costly so that invisibility functions as an aggravating factor rather than a liability shield. That shift a combination of two categories of solutions. The first is upstream, detection-first tools like verification rights with consequences, auditability-by-design via logging and monitoring, and robust whistleblower and audit infrastructure. The second is downstream, litigation-facing reforms that prevent information asymmetry from becoming immunity, like narrow early information-forcing, concealment-sensitive presumptions and tolling, and legislative recognition of certain "invisible" injuries as actionable. These tools are not substitutes for one another, but complements. Monitoring and audits generate reliable signals. Litigation supplies public factfinding, redress, and reputational accountability. Both channels work only if the system is built to surface what wrongdoers would prefer to keep unseen. At the same time, detection must be implemented with discipline and limits. Risk-based scope, minimization, confidentiality, and independent oversight must prevent the cure for invisibility from becoming a new regime of indiscriminate surveillance.

The stakes of incognito consumer harm 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. This trend will simultaneously intensify a race to the bottom, penalizing transparent firms while rewarding wrongdoers who profit by deliberate concealment. A legal system built for visible injuries can remain credible in such a world only if it stops treating invisibility as a mere practical inconvenience and starts treating it as the core wrong. The law cannot deter what it cannot reliably find, and it cannot preserve meaningful consumer autonomy if it continues to equate "no outward trace" with "no harm." The answer is to make concealment unprofitable, so that the incognito playbook is not a route to impunity, but a trigger for accountability.