KSTARR Enterprises, LLC

Negligent Digital Architecture™ (NDA²)

How system design enables exploitation, misleads users, and institutionalizes harm

By Katherine Starr

The Invisible Design That Shapes Harm

Consider the role of an architect in the physical world. An architect is not responsible for who is invited into a house that is the decision of the owner. Nor are they responsible for how a tenant uses the space. But the architect is responsible for designing a structure that will not collapse, that won't trap someone in a fire, that won't allow harm to occur because of a flaw in its physical form. The load-bearing calculations must be accurate. The roof must not leak. The walls must shield occupants from external harm. These are structural obligations. They are not contingent on who uses the building but are essential to its ability to function safely at all.

In this analogy, the digital equivalent of the owner installing keycards or assigning permissions reflects what we define in Negligent Digital Access™[1] (NDA¹). Those are access-layer controls—like logins, verification, or authentication protocols. They determine who gets in and under what terms. But if the building itself is structurally unsound if the windows don't function, if a room collapses under normal use, if entering a certain part of the building exposes you to avoidable danger then the fault lies with the architect, not the user or the access policy.

This is what Negligent Digital Architecture (NDA²) identifies. Platforms are being constructed with systems that are known to fail. If a digital environment allows phishing scams, permits phone spoofing, and actively suppresses legitimate user activity without recourse, those are not simply moderation choices. They are design flaws designs that reflect a foreseen risk. Just as car manufacturers are held liable for knowingly releasing vehicles with systems that fail under foreseeable conditions, digital platforms must be held to the same standard. The harm here is not speculative. It is the outcome of architectural choices made with full knowledge of their consequence.

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

That responsibility falls to the management of the building and, in digital systems, to the companies that design and deploy the platforms we use every day.

The modern internet is increasingly governed not by content alone, but by architecture. Every action taken by a user is routed through systems designed by trillion-dollar corporations whose products define the experience of access, expression, and trust. These systems are not neutral. They are structured, scaled, and monetized in ways that routinely mislead users, suppress truth, and invite harm[2]. The theory of Negligent Digital Architecture (NDA²) identifies these structural decisions as a central vector of digital harm.

Unlike visible acts of moderation or policy enforcement, NDA² functions in silence. It does not notify, explain, or engage. It simply permits harm to occur by omission, by delay, by misdirection and then assigns blame to the user for trusting the system it built.

This theory builds upon the foundational framework of NDA¹, which analyzes how platforms permit unauthorized actors to interface with users under false pretense or authority. That theory centers access as the harm vector, focusing on the decision to grant or deny entry and how platform design permits impersonation, manipulation, and unauthorized reach. It introduced the concept of the digital stack a layered infrastructure where harm is created and reinforced from the moment of interaction.

NDA² is the architecture of contradiction: where structure enables harm, silence enforces compliance, and the rules only apply to those who follow them. The harm is not abstract. It is systemic. It is known. And it is preventable.

This is not about bad content or bad actors alone. It is about a system that allows known fraud to persist while silencing expertise[3]. When scammers are permitted to spoof a platform's identity and send phishing messages with no restriction while a verified expert's bio is silently suppressed for using accurate terminology about sexual abuse and misconduct the platform does more than misfire. It codifies the wrong target. It institutionalizes the wrong response. And it operationalizes harm under the guise of protection.

Theoretical Framework: NDA² Compared to NDA¹ and Negligent Dating

NDA² builds on the foundation laid by NDA¹, which aligns with negligent hiring. NDA¹ focuses on who is allowed into the system highlighting failures at the point of entry, such as unverified or malicious actors gaining access to users through inadequate screening or credentialing.

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

NDA², by contrast, focuses on what the system allows once entry has occurred. It draws a direct line to defective product design: the system is functioning, the access point was granted, but what unfolds within the platform is governed by architecture one that predictably enables harm.

This theory also separates itself from Negligent Dating, which parallels negligent supervision. Negligent Dating addresses platforms that have no design framework at all no protocols for safety, no vetting structure, no accountability model. The absence of architecture is the architecture. In NDA², however, structure is present it is just engineered to fail under foreseeable conditions, or worse, to selectively enforce in ways that mislead users and shield platforms from liability.

The legal strategy advanced in Herrick v. Grindr[4] echoes this logic. The plaintiff in that case didn't argue that Grindr published harmful content he argued that Grindr's product design allowed impersonation, harassment, and stalking to continue after more than 50 reports. The harm wasn't user-generated; it was system-permitted. While the case was dismissed under Section 230, it opened the door to a new argument: that platform architecture, not just content, can be the source of liability.

NDA² formalizes and advances that argument. It states:

This legal evolution, as seen in Herrick v. Grindr, illustrates a shift in framing harm—not as content, but as consequence of product design. NDA² builds on this foundation but goes one step further: it does not merely assert that harm was allowed to occur. It argues that harm was built in.

In any other industry, this would be classified as a structural failure.

There are established international safety standards for physical products such as ISO 26262[5] in the automotive sector or ISO 9001[6] for quality management. These systems exist not because failure is guaranteed, but because it is foreseeable. A car must pass a structural integrity test before it can be sold. A product must not enter the market if its known flaws could endanger the user. Harm is prevented at the design level, not merely responded to after the fact.

But in the digital environment, no such standard exists. Platforms can be deployed at global scale with no architectural safety requirements. No certification body demands proof of structural soundness before launch. And yet, these platforms affect behavior, identity, livelihood, and safety arguably with more reach than any single product ever sold.

This absence of oversight is what NDA² exposes. It is not simply the presence of harm but the predictability of that harm, and the platform's decision to release the structure anyway.

Just as the CE Mark[7] ensures that a product meets minimum European safety criteria before entering the market, digital systems must be held to equivalent standards of architectural

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

accountability. NDA² demands that we stop treating platforms as harmless containers and start recognizing them as engineered environments where silence, suppression, and spoofing are not unfortunate side effects, but outcomes of negligent design.

Architectural Harm in Action: How Design Codifies Risk

The harms this theory addresses are not theoretical. They play out daily across systems that claim to protect users.

When a verified expert attempts to publish a professional biography that includes accurate language about sexual abuse and institutional misconduct, and that content is silently suppressed without notice, this is not a content violation it is the outcome of a system built to over-enforce without transparency. The user did nothing wrong. The architecture chose to obscure rather than notify.

When that same user receives a phishing message posing as platform support during the precise window when their content has been hidden, the scam becomes effective not because the message is credible, but because the platform itself created confusion. The impersonator steps into the vacuum. The system made the fraud believable.

When a user in crisis searches for fire restoration, locksmith help, or airline support and is shown fraudulent call centers at the top of the search results while legitimate businesses are buried — this is not a content oversight. It is a monetized design. The system rewards ad revenue and placement over validation and public protection.

These harms were not accidental. They were allowed to persist by design.

Liability and the Fallacy of Blaming the User

NDA² is not a theory about harm occurring solely at the moment of abuse. It is about the systemic design decisions that make abuse inevitable long before any direct harm takes place. This is where it departs from platform liability models rooted only in content or moderation timelines.

In the consolidated federal litigation *In re: Uber Technologies, Inc., Passenger Sexual Assault Litigation*[8] (MDL No. 3084), over 1,600 plaintiffs allege that Uber's platform design failed to implement adequate safety measures, such as proper driver screening and in-app emergency features, despite being aware of the risks. Similarly, in *In re Lyft Inc Derivative Litigation*[9], shareholders accused Lyft's leadership of neglecting passenger safety, leading to a settlement that included commitments to enhance safety protocols and governance reforms. These omissions

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

highlight features typically associated with Negligent Dating™: an absence of safety frameworks, vetting structures, and user protections.

NDA² advances that reasoning. It clarifies that when a platform's structure is built in a way that systematically allows these failures even while actively policing neutral or protective speech the design itself becomes the source of liability. The issue is not merely what the platform fails to remove, but what it was designed to permit, ignore, or incentivize.

While these deficiencies underscore a failure to build for safety, NDA² identifies a distinct harm: it is not simply the absence of design, but the presence of design choices that permit foreseeable abuse. The negligence is not in omission alone it is in the architecture that systematically allows repeat scams, impersonations, suppressions, and delayed or absent recourse to persist. It is the system's structure itself that becomes the mechanism of harm.

The distinction is simple but foundational: the abuse does not begin at the point of contact. It begins with the design choices that made that contact and the system's silence around it possible in the first place.

If you build a roof that leaks, you know that when it rains, the water will enter the structure. You know it will damage the ceiling, warp the floors, encourage mold, and potentially compromise the integrity of the entire building. This is not a surprise. It is a foreseeable outcome of a design flaw. And yet, in the digital context, the platforms argue as if the "rainfall itself" i.e. the predator, the abuser, the scammer, the impersonation, the phishing link is the user's burden to bear, rather than acknowledging that the system was built with a leaky roof.

This is the core distinction of NDA². When the technology stack is built with known vulnerabilities whether it's spoofable communication, unauthenticated authority signals, or opaque moderation systems then the harm that follows is not incidental. It is engineered into the design. Blaming the user for "getting wet" is not just disingenuous it's negligent.

In no other industry would we tolerate a structure that fails under normal, foreseeable conditions and then excuse that failure as the responsibility of the occupant. But in digital architecture, platforms deflect responsibility for their own design logic by pointing to the weather, the user, or the attacker anything but the leak they built and failed to fix.

The Path Forward: Accountability in the Age of Infrastructure

We do not allow buildings to collapse and blame the people standing inside. We do not allow vehicles with known brake defects to stay on the road. We require that cars with electronic and software systems comply with strict safety protocols, such as ISO 26262, which mandates functional safety in automotive environments ensuring that defects are identified and addressed long before the vehicle ever reaches a driver.

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

We do not allow children's toys to bypass safety testing. We do not tolerate household appliances that catch fire due to known wiring flaws. In every other sector, product safety is a prerequisite, not an afterthought. And yet, in digital systems where architecture governs identity, communication, and trust no equivalent protections exist.

Having worked within the business sector of a global certification body that audits compliance with ISO and CE standards across multiple industries, I gained a clear understanding of how rigorous, standardized design review protects consumers an accountability model starkly absent in digital architecture today.

There is no ISO-equivalent for interface safety. No CE Mark for platform design. No UL review for algorithmic logic. Platforms can scale globally, enable fraud, suppress truth, and endanger users without a single required structural review before launch.

And every piece of the digital structure matters. In the physical world, the Takata airbag disaster[10] stands as a grim reminder: one defective component used across dozens of car models—led to the largest automotive recall in history, multiple deaths, and the complete financial collapse of the company. The fault wasn't in the car as a whole, but in a single embedded system that was allowed to fail. That's the standard we accept elsewhere: every part must meet scrutiny, because known risk is never neutral.

In tech, however, not only are these flaws unregulated they're often monetized. Entire business models

have emerged that either:

- Profit from the harm directly (through platform structures that reward disinformation, manipulation, or fraud), or
- Charge users to repair reputational damage or remove harmful content that never should have been permitted in the first place[11].

An entire industry has emerged from the predictable failures of negligent digital architecture. Companies are formed specifically to profit from the aftermath of harm a clear indicator that the harm originates not from random misuse, but from structural design flaws.

These business models depend on offering services such as privacy protection for data leaked through vulnerable systems, reputational repair following spoofing or impersonation, and content removal only after damaging exposure has already occurred.

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

Each of these services exists because the architecture failed. They are not solutions—they are market responses to known, preventable failures. And every one of them is a direct result of a Negligent Digital Architecture (NDA²) breakdown.

These are not safeguards. They are aftermarket remedies for architectural failure—services sold back to the very users the system failed to protect in the first place.

Yet in tech, there is no legal doctrine that has evolved to treat these failures as product liability, despite meeting all traditional thresholds: foreseeability, failure to warn, defective design, and measurable harm.

It is not enough to retroactively remove harmful content. When platforms are deployed with full knowledge of structural vulnerabilities such as spoofable communication, silent suppression, or opaque enforcement the harm is not incidental. It is engineered. And it must be treated as a design defect, not a moderation failure.

NDA² demands a fundamental shift:

- From reactive moderation to architectural accountability.
- From blaming users to certifying systems.
- From platform immunity to product liability—when harm is caused by the very structure that allows it to thrive.

The models already exist. Building codes. Automotive safety protocols. Consumer product regulations. Each one is built on the idea that harm is preventable when risk is known. The internet must no longer be the exception to that rule.

The structure is the harm. And the legal system must evolve not to invent a new doctrine but to apply the one we already have.

We call it product liability. It exists precisely to assign responsibility when design defects cause foreseeable harm. It's time to extend that standard to the digital structures that now govern our lives. These platforms are not exempt because they are intangible. They are products. They are systems. And they are failing by design.

Because scale cannot be an excuse. Silence cannot be a shield. And platforms cannot be the only industry allowed to harm the public by design.

The structure is the harm. It is time to hold it accountable.

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

Citations and Attributes

APA (7th Edition):

Starr, K. (2025). *Negligent digital architecture: How platform design codifies harm*. KStarr Enterprises, LLC. https://www.katherinestarr.com/negligent-digital-architecture/

MLA (9th Edition):

Starr, Katherine. *Negligent Digital Architecture: How Platform Design Codifies Harm*. KStarr Enterprises, LLC, 2025. www.katherinestarr.com/negligent-digital-architecture/.

Bluebook (Legal):

Katherine Starr, *Negligent Digital Architecture: How Platform Design Codifies Harm*, KStarr Enterprises, LLC (2025), https://www.katherinestarr.com/negligent-digital-architecture/.

---

[1] Starr, K. (2025). Negligent digital access: When platform design enables harm. KStarr Enterprises, LLC. https://www.katherinestarr.com/negligent-digital-access/
[2] Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
[3] Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.
[4] *Herrick v. Grindr LLC*, 765 F. App'x 586 (2d Cir. 2019).
[5] International Organization for Standardization. (2018). *ISO 26262: Road vehicles – Functional safety*. Geneva, Switzerland: ISO.
[6] International Organization for Standardization. (2015). *ISO 9001: Quality management systems – Requirements*. Geneva, Switzerland: ISO.
[7] European Commission. (n.d.). CE marking – Conformity assessment. Retrieved from https://ec.europa.eu/growth/single-market/ce-marking_en
[8] *Uber Technologies, Inc., Passenger Sexual Assault Litigation* (MDL No. 3084, N.D. Cal. 2023)
[9] *Lyft Inc. Derivative Litigation*, No. CGC-20-584549 (Cal. Super. Ct., S.F. Cnty., filed Feb. 19, 2020)
[10] National Highway Traffic Safety Administration (NHTSA). (2023). *Takata airbag recalls*. U.S. Department of Transportation. https://www.nhtsa.gov/equipment/takata-recall-spotlight
[11] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

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