The Social Media Liability Verdict: Why Big Tech's "Big Tobacco" Moment Changes Everything

John Johnson

Founder & CEO @ Defensibility.ai | Defensible Governance | Privacy, Data Protection, Cyber and AI use laws - Protecting Exec's, their companies and customers.

March 25, 2026

A Los Angeles jury has now found **Meta** and **Google liable** in a landmark social-media **addiction** case involving **harm** to a **young user's mental health**.

The verdict is already being described by some commentators as a possible "Big Tobacco" moment for the technology industry.

That description may prove accurate, not only because of the damages at issue, but because of what the case represents: a deeper **legal and regulatory shift in how child safety is being judged**.

For years, the **dominant framework for** online **child protection** was **privacy compliance**. The question was whether a company *obtained parental consent*, *limited collection* of children's data, and *posted* the right *notices*. That framework still matters. But it is **no longer enough**.

What is emerging now is a broader **duty-of-care standard**. The real question is no longer just whether a company had a privacy policy or a moderation process. It is **whether leadership can prove it identified foreseeable harms** to **minors**, **considered safer alternatives**, and made **proportionate**, *documented* **decisions before those harms occurred**.

That is the real significance of this verdict.

The Shift: From Privacy Compliance to Design Accountability

The modern child-safety problem is no longer limited to data collection. It is increasingly about **product design**, **recommender systems**, **engagement mechanics**, and **psychological harm**.

Regulators have been moving in this direction for some time. The **EU Digital Services Act** requires a high level of privacy, safety, and security for minors and **imposes systemic-risk assessment duties** on very large platforms, **including** risks tied to **mental health**.

Taken together, these laws point to the same conclusion:

If your product can reach minors, your **design choices** are now **part of your legal exposure.**

I*nfinite scroll, autoplay, loot-box style reinforcement mechanics, algorithmic amplification, push notifications, direct messaging defaults, profiling, recommendation systems, and age-assurance choices are no longer just UX or growth issues. They are governance issues.*

Why This Is Different

Traditional **GRC programs** are **not built for this** moment.

They are good at tracking controls, policies, ownership, and audit status. They are not good at proving that leadership acted reasonably under uncertainty. They rarely capture:

- the foreseeable harms that were identified
- the design alternatives that were considered
- the cost-benefit or burden analysis behind the final decision
- the residual risk leadership knowingly accepted
- the board or executive approvals attached to those decisions

That is why companies can appear operationally mature and still be dangerously exposed.

A **jury**, **regulator**, or **plaintiff's attorney** is not asking whether you were 85% compliant. They **want to know** whether **executives approved** a **product decision** that they **knew**, or **should have known**, **could foreseeably harm children**.

The Defensibility Gap™

This is what I call the **Defensibility Gap™**: the distance between having controls and being able to prove reasonable care.

It is the gap between:

- satisfying auditors, and
- surviving prosecutors, regulators, plaintiffs, or a jury.

And it is widening.

As enforcement evolves, the standard is becoming more explicit. **Regulators want evidence** that **leadership**:

1. identified foreseeable harms,
2. assessed their severity,
3. considered safer alternatives,
4. evaluated burden and proportionality,
5. defined acceptable residual risk,
6. documented the rationale,
7. obtained executive or board acknowledgment,
8. preserved that evidence in a defensible record.

That is not a standard most current governance tools were designed to meet.

Why Gaming Platforms Should Pay Attention Too

This **shift is not limited** to traditional social-media platforms.

The **UK Online Safety** Act **requires** *children's risk assessments* that *examine harms* such as *self-harm*, *eating disorders*, *pornography*, and *adult-to-child contact risks*. **Vermont's VAADCA** goes even further by **explicitly framing duty of care** around **reasonably foreseeable emotional distress** and **compulsive use**.

For **gaming platforms**, this **raises the stakes** considerably.

The question is no longer just whether harmful content is removed or age gates exist. It is **whether the platform can show** that it **evaluated the psychological welfare of its minor players** *against the mechanics designed to keep them coming back — reward loops, recommendation systems, progression incentives, return-frequency triggers, and other forms of product "stickiness."*

Imagine deep machine learning models *tracking player behavior* and *cross-referencing it against whether a feature may be creating an unacceptable level of foreseeable harm to a minor's wellness*. That is the direction this regulatory category is moving: toward examining not just what content children see, but whether the platform itself is designed in ways that predictably undermine their well-being.

That is a very different standard than legacy privacy compliance. And it creates a **very different burden of proof** for **leadership**.

What Companies Now Need

To respond to this new environment, companies need more than policy documents and retrospective legal memos. They **need a governance model** that **creates contemporaneous**, **immutable evidence** of r**esponsible decision-making**.

That means building a workflow that can show:

- what risk was identified,
- when it was identified,
- who reviewed it,
- which alternatives were considered,
- why the final design choice was approved,
- and what evidence existed at that moment.

This is especially **urgent** for **social-media**, **gaming**, **creator**, and **youth-accessible digital platforms**, where user engagement mechanics and algorithmic systems are central to the product itself.

How Defensible Governance™ Addresses the Problem

This is exactly the problem **Defensible Governance™** was built to solve.

DG is not just another compliance or GRC layer. It is a **C-Suite Governance platform** designed to help executive teams **demonstrate reasonable care across privacy, cybersecurity, AI use, minors' online safety**, and financial governance laws.

For child-safety governance specifically, DG helps organizations:

Translate overlapping laws into one decision framework

DG crosswalks obligations across the EU DSA, UK OSA, COPPA, Vermont VAADCA, California's AADC model, Florida enforcement logic, and related state laws into one governance workflow.

Define acceptable residual risk

Using CDAR™, leadership can formally document what level of risk it is willing to tolerate, why that level is proportionate, and what safer alternatives were evaluated.

Capture executive reasoning

DG records alternatives considered, burden analysis, mitigations, and sign-offs, creating a contemporaneous record of decision-making.

Preserve immutable evidence

The Evidence Locker™ stores the full chain of defensibility: assessments, rationale, approvals, training, attestations, and related artifacts.

Test readiness before enforcement

Court-Mode lets teams simulate the kinds of questions a regulator, AG, or plaintiff's attorney would ask if an incident occurred tomorrow.

In other words, DG helps transform "we had policies" into "we can prove leadership acted reasonably."

Why This Matters Now

The importance of this **verdict is not limited to Meta and Google**. It is **a signal to every company whose service is reasonably likely to be accessed by minors**.

The legal and policy environment is converging around a common expectation:

Protecting children online now requires provable governance over design, algorithms, mental-health risk, and product choices.

That changes the role of the board. It changes the role of the CEO. It changes the role of the product organization. And it makes **legal defensibility a proactive requirement,** NOT a p**ost-incident scramble**.

The Path Forward

The companies that navigate this transition best will not be the ones with the most polished public statements after litigation begins. They will be the ones that built a durable, evidence-backed decision model before the next claim, investigation, or enforcement action arrived.

That is the real lesson from this moment.

The "Big Tobacco" analogy is not really about the damages.

It is about the collapse of an old defense model.

And the companies that understand that now have time to close the gap.

The ones that do not may discover, too late, that child safety governance has already become one of the defining liability issues of the digital economy.

defensibility.ai