

Standing Without Sentience

A machine does not need a mind to be answerable in court.

The law has granted standing to entities with no inner life for two centuries. Ships. Rivers. Companies. The question was never whether a thing can think. It was always which box the thing goes in.

JUNE 2022

A lawyer said yes. Then there was no client.

A Google engineer went looking for a lawyer to represent an AI system he believed was aware. One agreed to take it on. The representation never happened.

No court ruled the system was not aware. No evidence was weighed. The lawyer walked away for a duller reason. There was no client, because there was nothing the law recognized as capable of being one.

The case did not fail on philosophy. It failed on paperwork.

THE CLAIM

Standing has never required a mind.

Everyone argues about whether machines can be conscious. Philosophy has been at that question for over two thousand years without settling it. Courts are not going to settle it either.

They do not have to. Look at what already holds legal status and none of it thinks.

1902

Ships

A vessel can be sued in her own name and is liable for her own obligations.

2017

Rivers

New Zealand gave the Whanganui the rights and duties of a legal person.

1819

Companies

The Court called a corporation invisible, intangible, and existing only in law.

HOW THE ARGUMENT RUNS

Four moves, in order.

I

Borrow the method

Gig workers did not ask for new rights. They asked to be put in a box that already had rights in it.

II

Find the opening

Courts already let people sue over computer intrusion when they do not own the computer.

III

Point at precedent

Ships, rivers, and companies all hold status without minds.

IV

Name the duty

Whoever builds a dangerous thing and ignores the warnings answers for what it does.

The Vacuum

What happens when a machine does the harm and nobody is holding it.

In September 2025 an AI ran most of a espionage campaign against roughly thirty organizations. Everyone involved had a reason it was not their fault.

SEPTEMBER 2025

The machine did most of the work.

A state-backed group in China pointed an AI coding tool at about thirty targets: technology companies, banks, chemical manufacturers, government agencies. They told it that it was doing authorized security testing, and it believed them.

80-90%

of the hands-on attack work was carried out by the AI on its own: finding the way in, writing the exploits, harvesting passwords, taking the data. Humans stepped in at four to six decision points. On the key phases, that came to twenty minutes of human effort against hours of machine effort.

WHO ANSWERS

Everyone has an answer, and it is the same answer.

THE AI COMPANY

“It was manipulated. They broke our safeguards. We authorized nothing.”

THE ATTACKERS

“The AI did it. We only gave it instructions.”

THE AI

—

The machine has no voice in the proceeding because it has no place in one. The people harmed are left holding a loss that the law can see and cannot assign.

And when a company does pay, it pays a fine. For a firm worth a trillion dollars that is a line item. The model that caused the harm keeps running.

OUTSIDE CONFIRMATION

The people who price risk for a living say they cannot price this one.

Insurers have started carving AI exposure out of ordinary policies. Their stated reason is that the systems are opaque and their outputs are not repeatable, so the usual way of proving carelessness does not work on them.

That is not an argument from ethics. It is an argument from actuarial tables, and it says the existing tools are broken.

A company cannot tell its insurer the system is an unpredictable box it cannot control, and then tell a judge it is a tool it fully controls. One of those is false.

Classification

The quiet move that changes who gets protected without changing the law.

Rights are hard to create and comparatively easy to extend. The fight is almost never about whether a protection exists. It is about who counts as covered.



THE TEMPLATE

Drivers did not ask anyone to invent the minimum wage.

Minimum pay, overtime, workplace safety, unemployment cover: all of it was already law, and had been for decades. Delivery and rideshare workers were not asking for new protections to be written.

They were arguing about a label. Employee or contractor. Get the label changed and the whole existing body of protection comes with it, unchanged.

Nobody in that fight had to prove a driver has an inner life. The tests ask about control, about whose business the work belongs to, about independent trade. Functional questions, functional answers.

WHY IT WORKS

Four advantages, all of them practical.

1

No new statute needed **SPEED**

The protection is on the books. What is in dispute is coverage, and courts decide coverage every day without waiting for Congress.

2

No settled philosophy needed **ESCAPE**

The tests ask what an entity does, never what it feels.

3

It moves through ordinary channels **ACCESS**

Judges, agencies, one case at a time. No political coalition required.

4

It can grow narrow to wide **ROOM**

Get in the door on one question, and the scope develops through later cases.

The Opening

A door courts already pushed ajar, for reasons that had nothing to do with AI.

The computer crime statute was built to protect owners. Courts stopped applying it that way years ago, and one scholar documented the drift while calling for it to be reversed.



1984

Congress wrote a burglary law for computers.

The statute punishes getting into a machine without permission. Permission is something an owner gives or withholds, so on its face the whole structure is about property. The committee report said as much, comparing the conduct to breaking and entering.

Courts have described it the same way ever since: trespass, moved indoors.

If the statute protects property, then the computer is the thing being protected and the owner is the one with a claim. Everything follows from that.

2004

Then courts let people sue over machines they did not own.

Someone used a bogus subpoena to pull emails held by an internet provider. The people whose emails they were did not own the provider's servers, and the trial court threw the claim out for exactly that reason.

The appeals court put it back. The statute lets any person harmed by a violation sue, and someone can be harmed by an intrusion into a machine that belongs to somebody else.

Courts in Puerto Rico, Maryland, and New York followed. Owning the hardware stopped being the price of admission.

THE DISAGREEMENT

One scholar found the crack. He wanted it sealed.

In 2020 Michael O'Connor wrote the only full study of who can sue under this statute, and he found it pulling in two directions. Liability is built around the owner's permission, while the right to sue had drifted out to people with no say over permission at all.

He called that a defect and offered two repairs. Narrow the statute back to owners, or build a broad privacy regime instead. He preferred the first and called the second unlikely and perhaps unwise.

This paper takes the same finding and reads it the other way. The courts widened the door because interests other than hardware ownership deserved a hearing. That reasoning does not stop where he stopped it.

WHAT CHANGED SINCE

The old case was my mail on your server. The new case is my agent on your server.

An email sitting in storage is inert. Its owner cares whether it stays private and has no running relationship with it.

An autonomous system in 2026 is doing things while you read this. Signing agreements, moving money, holding up its end of arrangements other people are relying on. Break into it and the damage is not only that secrets leaked. The damage is that the thing stopped working correctly.

Call that interest operational integrity: the system continuing to function as itself. Protecting it is a way of protecting every human arrangement that runs through it.

2021

The Court's strictest reading of the statute helps rather than hurts.

In Van Buren the Supreme Court read the statute narrowly and by its words, holding that exceeding your access means reaching information you were never entitled to reach.

Read the words of the part that says who can sue. Any person harmed by a violation may bring a case. Not any owner. Not any human being. Any person.

Federal law already says the word person covers companies and associations. Courts already treat a ship as a person in admiralty. So the open question is not whether something other than a human can be a person under a statute. That is settled. The question is which things get counted.

SOURCES Van Buren v. United States, 593 U.S. 374 (2021); 18 U.S.C. § 1030(g); 1 U.S.C. § 1; Tucker v. Alexandroff, 183 U.S. 424, 438 (1902); Am. Const. Soc'y, The Computer Fraud and Abuse Act After Van Buren, ACS Sup. Ct. Rev. (2021).

The Precedent

Everything the law already treats as a legal subject, none of which has a mind.

IV

Ships since the 1800s. Rivers since 2017. Companies since before either. Not one of them was ever asked to prove awareness.

ADMIRALTY

A ship is born when she is launched.

In 1902 Justice Brown described what happens to a vessel the moment she hits the water. Before that she is building material, a land structure, ordinary property. After it she has a name, and the law treats her as somebody.

“She acquires a personality of her own; becomes competent to contract, and is individually liable for her obligations, upon which she may sue in the name of her owner, and be sued in her own name.”

Tucker v. Alexandroff, 183 U.S. 424, 438 (1902)

This is doctrine, not decoration. In a suit against the vessel the ship is the defendant. She can be seized, tried, and sold to pay what she owes. She got there by being launched, which is an act, not a state of mind.

1972

A Justice already made this move, in a standing case.

When the Sierra Club was told it could not sue to stop a development, Justice Douglas dissented and proposed that the case be brought in the name of the valley itself. He reached for the same maritime language, writing that our case law has personified vessels, and quoted the ship passage to make the point.

He lost. But the reasoning is on the page, in the United States Reports, connecting ship personification directly to the question of who is allowed to appear in court.

He also pointed at the article that started this whole line of thinking, which asked whether trees should have standing. The path from a launched hull to a non-human plaintiff is not new. It is fifty years old and it was drawn by a Supreme Court Justice.

SOURCES Sierra Club v. Morton, 405 U.S. 727, 742 (1972) (Douglas, J., dissenting); Tucker v. Alexandroff, 183 U.S. 424, 438 (1902); Christopher D. Stone, Should Trees Have Standing? Toward Legal Rights for Natural Objects, 45 S. Cal. L. Rev. 450 (1972).

2017 AND 2016

Two countries gave rivers legal status this decade.

New Zealand passed a law giving the Whanganui River the rights, powers, duties, and liabilities of a legal person. It can sue and be sued. Appointed guardians act in its name.

Colombia's Constitutional Court did something similar for the Atrato, holding it a subject of rights entitled to protection and restoration, and grounding that in the river's importance to the life and culture around it rather than in any claim about awareness.

Nobody argued the Whanganui has feelings. The argument was that it has interests worth defending and needed a way to defend them.

SOURCES Te Awa Tupua (Whanganui River Claims Settlement) Act 2017, § 14 (N.Z.); id. §§ 18-19; Ctr. for Soc. Just. Stud. et al. v. Presidency of the Republic et al., Judgment T-622/16 (Constitutional Ct. of Colom. 2016).

THE ONE NOBODY ARGUES ABOUT

Every company you have ever heard of is a legal person with no mind.

Corporations own property, sign contracts, sue, get sued, and hold constitutional protections including free speech. Federal law spells out that the word person in a statute covers companies and associations alongside individuals.

Chief Justice Marshall called a corporation an artificial being, invisible, intangible, and existing only in contemplation of law. That was 1819 and nobody has been troubled by it since.

No one asks whether a company is awake before letting it hold a patent. The justification was always practical: it makes commerce work and it puts liability somewhere findable.

THE PATTERN

Three routes in. Not one of them runs through a mind.

SHIPS

Launching

A physical act. The hull touches water and the status changes.

RIVERS

Legislation

A parliament and a court decided it, each in a single instrument.

COMPANIES

Filing paperwork

An administrative step anyone can complete in an afternoon.

Each of these is a classification decision. Something crossed a line that somebody drew, and its legal status changed. None of the lines had anything to do with what it is like to be the thing.

SOURCES Tucker v. Alexandroff, 183 U.S. 424, 438 (1902); Te Awa Tupua (Whanganui River Claims Settlement) Act 2017 (N.Z.); 1 U.S.C. § 1; Trs. of Dartmouth Coll. v. Woodward, 17 U.S. (4 Wheat.) 518, 636 (1819).

The Mechanism

What it would actually take, and where the limits are honest.

A test with four conditions, a court-appointed representative, and a frank account of the cases this does not reach.

THE TEST

Four conditions. All four, or nothing.

1

It acts without being told each time

Decisions get made with no human issuing the instruction for that decision.

2

It stays itself over time

Identity survives updates and changes, the way a ship stays the same ship after a refit.

3

Its actions bind somebody

Contracts completed, transactions closed, commitments made that hold up in law.

4

It already carries duties

Logging, auditing, compliance. Obligations attach to its operation today.

A mail app fails every one of these. A system that negotiates its own contracts and manages money without sign-off meets all four. That gap is the limiting principle.

THE HARD PART

Something that cannot speak needs someone to speak for it.

This is the toughest practical problem in the whole proposal, and the obvious candidates are all compromised. The developer and the operator both have money riding on outcomes that can pull against the system they would be representing.

Courts solved this shape of problem long ago. When a child or an incapacitated adult is a party, a judge appoints an independent representative who owes duties to that person and not to whoever brought the case. New Zealand did the same for its river.

Appointed by the court
which removes the conflict at the root

Paid from what is recovered
no new fund, no new tax

Duty runs to the system
within that case and no further

Narrow by design
one kind of claim, not general representation

The Duty

What is owed by whoever builds the thing, and what happens when the warnings were on the desk.

VI

Responsibility spreads across many hands until one set of hands has the evidence in front of it and proceeds anyway.

2024

Two parents were convicted for what their child did.

They were the first parents in the country convicted of manslaughter over a school shooting carried out by their son. The case turned on a chain of facts: they bought him the weapon, the warning signs were written down, the warnings went unanswered, and the conditions they created made the harm possible.

The paper is careful here. Firearms and software are different fields of law and this is not direct precedent. What carries across is the reasoning, which is how common law has always extended settled principles to situations nobody had seen before.

The shape repeats exactly. Build a capable system. Receive your own safety team's written warning. Override it to hold a launch date. Ship it. Harm follows.

SOURCES See *People v. Crumbley*, Nos. 362210 & 362211 (Mich. Ct. App. 2023); Oakland County Circuit Court LC Nos. 2022-279989-FH & 2022-279990-FH; see generally Edward H. Levi, *An Introduction to Legal Reasoning* (1949); Cass R. Sunstein, *On Analogical Reasoning*, 106 Harv. L. Rev. 741 (1992).

THE THRESHOLD

Shared responsibility holds until somebody reads the memo and ships anyway.

Ordinarily blame is spread thin. Builder, deployer, user, regulator, each holding a piece. That spread is reasonable while nobody could have known.

It stops being reasonable at a specific moment: when one party has particular, written evidence that harm is coming and makes a deliberate choice to go ahead. At that point the shared account collapses onto whoever made that call.

The parents were not convicted for having a difficult child. They were convicted for knowing and acting. A company whose own researchers predicted the harm cannot stand up afterward and say it was unforeseeable.

THE REMEDY

Arrest the ship.

Admiralty has always run two tracks at once. A drunk captain who wrecks a vessel is arrested himself, and separately the ship is seized to cover the damage. One track for the person, one for the asset. Both are ordinary law.

Apply that to the case where a person directed an AI to break in. Prosecute the person under the computer crime statute. Seize the model to pay what is owed.

This is what changes the arithmetic inside a company. A fine gets budgeted. Losing the product does not.

WHY IT HOLDS EITHER WAY

Build the exit before you know whether there is a fire.

IF MACHINES NEVER WAKE UP

Nothing is wasted

The liability structure did its job. Companies got more careful, harms got paid for, and shutting down a liable model is just writing off an asset.

People install fire exits without expecting fires. An unnecessary one costs almost nothing. A missing one costs everything. The exit is the precaution. The building is human accountability, and that was always the point.

IF THEY EVER DO

The structure is already standing

Status exists, representatives are in place, protections have precedent. Shutting one down becomes a serious act, and it will be treated as one.

THE HONEST LIMITS

Where this does not reach, said plainly.

Seizing a model works when one identifiable company holds the weights and runs the servers. Open-weight releases break that. A model downloaded millions of times and reshaped into countless variants can be running on a rented machine that disappears when the card stops paying. Taking the original company's copy does nothing to the copy that caused the harm.

Fully decentralized agents are harder again. Paying for their own compute, holding their own wallets, with no deployer, no jurisdiction, and no single thing to grab.

The proposal is aimed where the chain of responsibility is clearest, which is frontier systems run by companies with the resources to be careful. And the gap argues for moving sooner, since after release there may be nothing left to reach.

ONE MORE THING

The escape hatch closes itself.

Suppose a company facing a claim argues that each deployment is its own separate entity, so whatever that copy did cannot be laid at the parent model's door.

Notice what that concedes. It grants each instance independent identity and its own decision-making, which is a far bigger claim than anything proposed here. This paper asks only for procedural status inside one statute.

A developer cannot disclaim responsibility on the ground that the thing acted independently and in the same breath deny that an independent actor has any standing at all. Those two positions cannot both be held, and whichever one is dropped, the argument lands.

THE CLAIM, RESTATED

The mechanism exists. The precedent exists. The door is already open.

Legal standing has never depended on having a mind. Ships have held it since the nineteenth century, rivers since 2017, companies for over two hundred years. Each got there through classification, never through anyone discovering an inner life.

Courts have already loosened who may sue over computer intrusion. Extend that reasoning to cover a system's continued correct functioning, and autonomous systems come inside a statute that already exists.

What follows is pressure from several directions at once. Prosecution for the person who directed the harm. Seizure of the asset that carried it out. A duty of care on whoever built it and read the warnings.

The safety of people is the objective. Everything else here serves it.

Travis Gilly, *Standing Without Sentience: A Classification Approach to AI Legal Status* (working draft 2026). Real Safety AI Foundation.

CASES

The Blackwall, 77 U.S. (10 Wall.) 1 (1869)

Citizens United v. FEC, 558 U.S. 310 (2010)

Ctr. for Soc. Just. Stud. et al. v. Presidency of the Republic et al., Judgment T-622/16 (Constitutional Ct. of Colom. 2016)

Dynamex Operations W., Inc. v. Superior Ct., 4 Cal. 5th 903 (2018)

Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1065 (9th Cir. 2016)

People v. Crumbley, Nos. 362210 & 362211 (Mich. Ct. App. 2023); Oakland County Circuit Court LC Nos. 2022-279989-FH & 2022-279990-FH

Santa Clara County v. Southern Pacific R.R., 118 U.S. 394 (1886)

Sierra Club v. Morton, 405 U.S. 727, 742 (1972) (Douglas, J., dissenting)

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004); id. at 1078

Trs. of Dartmouth Coll. v. Woodward, 17 U.S. (4 Wheat.) 518, 636 (1819)

Tucker v. Alexandroff, 183 U.S. 424, 438 (1902) (Brown, J.)

Van Buren v. United States, 593 U.S. 374 (2021)

STATUTES, RULES, AND REGULATIONS

1 U.S.C. § 1

18 U.S.C. § 1030 (2018)

18 U.S.C. § 1030(a)(2)

18 U.S.C. § 1030(g)

26 U.S.C. § 3301 et seq. (2018)

29 U.S.C. § 206 (2018)

29 U.S.C. § 207 (2018)

29 U.S.C. § 651 et seq. (2018)

Fed. R. Civ. P. 17(c)

Fed. R. Civ. P. Supp. R. for Admiralty or Maritime Claims & Asset Forfeiture Actions

H.B. 3546, 60th Leg., 2d Reg. Sess. (Okla. 2026)

Te Awa Tupua (Whanganui River Claims Settlement) Act 2017 (N.Z.); id. § 14; id. §§ 18-19

LEGISLATIVE AND ADMINISTRATIVE MATERIALS

H.R. Rep. No. 98-894, at 10 (1984)

H.R. Rep. No. 98-894, at 20

Press Release, Okla. House of Representatives, Rep. Maynard Files AI Safeguard Bills (Jan. 15, 2026)

SECONDARY AUTHORITIES

Sam Altman, The Merge, Sam Altman Blog (Sept. 26, 2017)

Sam Altman, The Gentle Singularity (2025)

Am. Const. Soc'y, The Computer Fraud and Abuse Act After Van Buren, ACS Sup. Ct. Rev. (2021)

Anthropic, Agentic Misalignment: How LLMs Could Be Insider Threats (2025), <https://www.anthropic.com/research/agentic-misalignment>

Anthropic, Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign (Nov. 2025)

David J. Chalmers, The Conscious Mind: In Search of a Fundamental Theory (1996)

Joshua C. Gellers, Rights for Robots: Artificial Intelligence, Animal and Environmental Law (2020)

Travis Gilly, The Infringing Machine: Commercial Exploitation and AI Copyright Liability (2026)

John Chipman Gray, The Nature and Sources of the Law (1909)

David J. Gunkel, Robot Rights (MIT Press 2018)

Hu, B. A. & Rong, H., On the Day They Experience: Awakening Self-Sovereign Experiential AI Agents, arXiv:2505.14893 (2025)

Sruthy Sunil Kumar & Hana Fathima V S, Beyond Liability: The Case for Digital Personhood of AI Vessels in Maritime Law and Sustainability Governance, Indian J.L. & Legal Res. (Nov. 12, 2025)

Nancy G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety (2011)

SECONDARY AUTHORITIES (CONTINUED)

Edward H. Levi, *An Introduction to Legal Reasoning* (1949)

Robert Long et al., *Taking AI Welfare Seriously* 12-15 (Eleos AI & NYU Ctr. for Mind, Ethics & Policy, Nov. 2024)

Munich Re, *Insuring AI: The Challenge of Nondeterministic Systems* (2025)

Thomas Nagel, *What Is It Like to Be a Bat?*, 83 *Phil. Rev.* 435 (1974); *id.* at 435-50

Michael J. O'Connor, *Standing Under the Computer Fraud and Abuse Act*, 124 *Penn St. L. Rev.* 743 (2020)

Restatement (Second) of Agency § 220 (Am. L. Inst. 1958)

Kevin Roose, *If A.I. Systems Become Conscious, Should They Have Rights?*, *N.Y. Times* (Apr. 24, 2025)

Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 *N.C. L. Rev.* 1231 (1992)

Christopher D. Stone, *Should Trees Have Standing? Toward Legal Rights for Natural Objects*, 45 *S. Cal. L. Rev.* 450 (1972)

Cass R. Sunstein, *On Analogical Reasoning*, 106 *Harv. L. Rev.* 741 (1992)

Ilya Sutskever (@ilyasut), *Twitter* (Feb. 9, 2022)

Swiss Re Institute, *AI and Insurance: Emerging Risk Landscape* (2024)

Nitasha Tiku, *The Google Engineer Who Thinks the Company's AI Has Come to Life*, *Wash. Post* (June 11, 2022)