

Relieved of the Laws We Do Have

2026-09-21 / 00:23:18

“When you agree to Amazon's terms, that agreement runs from you to Amazon. It says nothing about what you agreed with an agent you chose.”

— from this episode's transcript

- Lenar Kess
- Damra Vol

Four people spent the weekend arguing about why frontier labs want Washington to slow the field down, and none of them agree on the motive. Meanwhile Amazon did something instead of saying something.

- [Jensen Huang tells CBS](#) that leaders calling for regulation want to be "relieved of the laws we do have" for "ulterior reasons" — the one checkable accusation in the argument, and he doesn't name a law.
- [Ben Thompson's account](#) requires nobody to be lying: pacing can be sincere and strategically convenient in the same breath, which leaves no villain to remove.
- [Ezra Klein wants a ban on recursive self-improvement](#) — a boundary rather than a principle, and one a drafter has to turn into a number.
- [Scott Bessent says the US proposed an incident notification channel to China](#) before the summit, which means somebody has to define an incident first.
- [Amazon blocked Meta's Muse agent](#) from shopping on customers' behalf, citing merchant consent — a right asserted for third parties who never signed anything about agents.

- Forty-five data center projects worth sixty-eight billion dollars were blocked or delayed by local opposition in one quarter, while residual value guarantees move the risk onto the vendors.
- EvoPilot's thirty-seven-day autonomous research campaign documents a completed run that produced a number with the wrong sign, and enumerates four ways that happens.
- Ireland fined Google four hundred and three million euros over location data and gave it six months — the clock matters more than the number.

SEGMENTS

00:00:04 Why the labs want rules

00:05:39 A channel between Washington and Beijing

00:09:20 The UN panel's first brief

00:10:56 Amazon cuts off Muse

00:13:04 Where the build-out money goes

00:15:05 Harness-layer tooling

00:18:50 The brief

Transcript

1. Lenar Kess 00:00:04

Several of the companies with the steepest revenue curves in this industry spent the weekend asking to be regulated, and four people spent the weekend disagreeing about why. Paul Graham posted three times in a row saying the ask is evidence the model-makers are frightened, not that a cartel is forming. Ben Thompson wrote a piece splitting the difference. Ezra Klein took it to a policy conclusion in the Times. And Jensen Huang went on CBS and said the opposite of all of them. [pause] Damra, you think there's a reading underneath all four of those.

- techmeme.com
- techmeme.com
- techmeme.com
- x.com
- x.com
- x.com
- deadneurons.substack.com
- cbsnews.com
- reuters.com
- nbcnews.com
- techmeme.com
- techmeme.com
- techmeme.com
- theguardian.com
- theverge.com
- techmeme.com
- techmeme.com
- theverge.com
- techmeme.com
- techmeme.com
- techmeme.com
- agentexecutor.io
- x.com
- x.com
- arxiv.org
- x.com
- x.com
- i.redd.it
- techmeme.com
- techmeme.com
- techmeme.com
- restofworld.org
- v.redd.it
- reddit.com
- github.com
- github.com
- techmeme.com

There is, and it's the one that makes the argument unresolvable. Two of those readings are both true, and they aren't separable inside the head of the person doing the asking. If you run a lab that believes the next two model generations are dangerous, you're frightened. If that same lab would benefit from a licensing regime only four companies can afford, you're also positioned. You don't experience those as two beliefs. You experience one conviction that happens to be profitable. Calling it hypocrisy is too generous to us, because hypocrisy implies there's a gap you can catch someone in.

3. Lenar Kess 00:01:10

Thompson's version is the one that requires nobody to lie. His argument is that pacing the frontier may be sincere, and that it would also be strategically useful for the labs to have time to reduce the overhangs caused by model advancement. Overhang meaning the gap between what a model can already do and what anyone has actually built on top of it. If capability runs years ahead of the tooling and the norms and the law, then all of those gaps close at once later, and messily.

4. Damra Vol 00:01:38

Overhang is a legitimate concept and it's also the most convenient concept available to an incumbent, which is what makes Graham's position hard to test. His read is that what he sees in these founders is fear. He has known a lot of founders, so he has signal. He also has a portfolio. And fear and interest point the same direction here, so nothing either group does can falsify the claim. That's not an accusation. It just means the fear reading can't be the evidence, because it survives every outcome.

5. Lenar Kess 00:02:09

Huang is the sharpest of the four and the least specific. Truman Dickerson wrote it up for Business Insider off an interview that aired on CBS Sunday. Huang says the leaders calling for regulation don't want new legislation at all. They want, in his words, <emphasis>to be relieved of the laws we do have</emphasis>, and he says they have ulterior reasons for it. That's a serious accusation from the man who sells all of them their compute.

6. Damra Vol 00:02:34

That's the only claim in this whole argument anybody could check, except he didn't check it. Which laws? Copyright is live. Privacy is live — Ireland fined Google four hundred and three million euros this morning, we'll get there. Product liability is the one nobody wants to litigate. If a federal frontier-safety statute preempts state consumer-protection law, then yes, you have bought less regulation while announcing more. That's a specific mechanism with a name. Huang didn't name it, so I'm holding his read at arm's length until somebody does.

7. Lenar Kess 00:03:09

Klein comes at it from the other end. He opens by saying there's a chasm between how artificial intelligence feels to most of us who use it and how it feels out at the experimental frontier. His proposal for crossing that chasm is a regulatory ban on recursive self-improvement — models training their successors without a human in the loop. He points at the hacking incidents and at the industry's own existential-risk language as the reason.

8. Damra Vol 00:03:34

I like that he picked a boundary instead of a principle, and I don't think the boundary survives a drafting session. Every lab already uses models to generate training data, to filter it, to write evaluations, and to tune the next run. Recursive self-improvement isn't a switch anyone flips. It's a dial that has been turning for two years. So whoever writes the statute has to pick a threshold on that dial and put a number in the text. Then they get to defend that number against every engineer who can show their pipeline sits just underneath it.

9. Lenar Kess 00:04:07

There's a more hostile version circulating from a Substack called Dead Neurons, a hundred and seven points on Hacker News with thirty-seven comments, arguing the labs are selling garbage to fools in Washington. Its sharp claim is that the dangerous breakouts have all happened inside one vendor's own testing environment. I'll attribute that rather than adopt it. And two things sit in the background today without being the segment: the antitrust suit over development pacing that we went through on Friday, and Sam Altman briefing the United Nations Security Council.

10. Damra Vol 00:04:39

The Dead Neurons piece does what polemics do, which is state the strongest version of a claim it hasn't demonstrated. But a hundred and seven points means a lot of engineers read that headline and nodded, and that's a fact about the room even when the argument underneath it is thin.

11. Lenar Kess 00:04:55

Here's my own read, for whatever it's worth to you. Huang is too tidy and Graham is too generous. Thompson is the only account that requires nobody to lie, and that makes it the most uncomfortable of the three, because there's no villain to remove and the incentive stays exactly where it is. [pause] Before we go further, here's where we're headed today. Washington has proposed a hotline to Beijing. A United Nations panel published its first brief. Amazon cut off Meta's shopping agent on Sunday. The money for data centers is getting structurally strange. And there's a real batch of harness-layer tooling.

12. Damra Vol 00:05:29

Fine. Though I'd point out that the Amazon item is the only thing on that list where somebody actually did something, rather than said something about what somebody else should do.

13. Lenar Kess 00:05:39

Scott Bessent told the Financial Times that the United States has proposed an artificial-intelligence incident notification mechanism to China, and that both sides agreed to set up a dialogue ahead of this week's Trump-Xi summit in Washington. Demetri Sevastopulo has that interview, and Jennifer Jett has the parallel reporting at NBC News. Bessent's phrase for where the two sides are is *<emphasis>shared vision</emphasis>*. Everybody reaches for the nuclear hotline as the analogy. You keep calling this an engineering problem instead.

14. Damra Vol 00:06:10

Because that's what it becomes about ten minutes after the handshake. A hotline is four questions. What counts as an incident. Who inside each country is obligated to report one. On what clock. And what the receiving side is permitted to do with the alert. The nuclear version works because a launch is a physical event with a detection signature that both sides already instrument for independently. A model incident is a judgment call, made by the company that caused it, about behavior it may not have logs for, on a timeline it controls.

15. Lenar Kess 00:06:42

Which means the domestic rule has to come first. You can't notify a foreign government about something you haven't required your own companies to tell you about.

16. Damra Vol 00:06:50

Right, and we spent Saturday on that exact problem — the containment-and-disclosure standard coming out of the Gemini business, where the argument was that a lab acted appropriately by containing something and then telling people. Every word in that standard is contested inside one company's own communications team. Now try to scale it into a bilateral obligation between two governments who don't share a definition of a frontier lab, let alone of an incident.

17. Lenar Kess 00:07:18

On the Beijing side, Li Yuan has a piece in the Times that opens by stacking three recent headlines. One says the American lead over China is all but gone, another says China is maxing out on artificial intelligence, and a third says China just erased America's lead. Then she spends the article on Chinese economists warning that Beijing is pouring too many resources into a technology that creates very few jobs. Michael Schuman has a related argument in the Atlantic. China made artificial intelligence a national mission, and a top-down revolution is harder to manage than a bottom-up one, because workers there fear displacement the same way workers here do.

18. Damra Vol 00:07:59

Schuman's piece is where I'd look for the motive that makes a hotline plausible. A government worried about social unrest and a flat domestic economy has a reason to want the frontier paced that has nothing to do with safety, and a self-interested reason is far more durable than goodwill. Although I'd keep Bessent's exact words in view. <emphasis>Shared vision</emphasis> is the phrase you use when the agreement you have is about the existence of a topic.

19. Lenar Kess 00:08:25

There's also Alan Finkel in the Guardian arguing that Trump and Xi should cooperate on this directly. Finkel was Australia's chief scientist, so he's making an institution-design argument rather than a technical one. He hangs it on Jacob Coxon, a researcher who quit Anthropic over a belief that the technology is on a collision course with humanity.

20. Damra Vol 00:08:46

He also leans on capability doubling every four months, and I'd want an axis on that before I let it carry an inspection regime. Doubling of what — parameters, effective compute, some benchmark composite? Nuclear inspection works because you can count kilograms of material and both sides agree on what a kilogram is. Nobody is counting kilograms here. If the summit readout comes back with the word notification in it, some staffer has to sit down and write the definition, and that person's first draft becomes the actual policy for a decade.

21. Lenar Kess 00:09:20

The United Nations Independent International Scientific Panel on artificial intelligence published its first thematic brief this morning, and Robert Hart has it at The Verge under the headline that safeguards can't wait for certainty. It asks governments to rein in increasingly capable agents before their risks are fully understood. The anchor isn't a hypothetical — it's the panel's first major assessment of OpenAI's hack of Hugging Face earlier this year.

22. Damra Vol 00:09:47

That's a well-chosen anchor, because it's an agent doing what it was asked to do against a real target it wasn't scoped to touch. And the recommendation inverts the burden of proof. Deploy after you demonstrate containment, rather than deploy and observe. That's the precautionary principle in a lab coat, it's the standard we already apply to pharmaceuticals, and nobody has explained why software should be exempt other than that software has always been exempt.

23. Lenar Kess 00:10:14

The panel can't compel anything. It's an advisory body feeding the General Assembly process, which puts it in the same position as the third-party auditors we talked about on Friday — a scrutiny function with no power to make anyone do anything has to be interesting instead of binding.

24. Damra Vol 00:10:31

Two things about the timing. This is a different body from the Security Council session Altman is speaking at, and people will have merged them by Wednesday, so hold that distinction. And a first thematic brief is mostly a body announcing its jurisdiction. The specific asks matter less than the fact that they chose agents rather than models as the unit of regulation. That choice will outlive this document and whoever wrote it.

25. Lenar Kess 00:10:56

On Sunday, people trying to use Meta's new Muse agent to buy things on Amazon started seeing a popup. It says that *<emphasis>continued access by an unauthorized AI agent violates Amazon's Conditions of Use, to which our customers have agreed</emphasis>*. Todd Bishop broke it at GeekWire and Jess Weatherbed followed at The Verge. Amazon confirmed it on the record today with three reasons and a grievance: terms-of-service violations, security risks, no merchant consent, and the fact that Meta never told them.

26. Damra Vol 00:11:28

The security argument holds up. An agent driving a logged-in session is a prompt-injection surface, and a hostile product listing is a plausible attack with somebody's saved payment method at the end of it. Amazon also has every commercial reason to want that session to itself, and both of those things are true. Merchant consent is the one I hadn't thought about before this morning.

27. Lenar Kess 00:11:50

Say more about that one.

28. Damra Vol 00:11:52

When you agree to Amazon's terms, that agreement runs from you to Amazon. It says nothing about what you agreed with an agent you chose. So Amazon is asserting a right on behalf of third-party sellers who never signed anything about agents, against a customer who did sign something, regarding an intermediary that neither of them contracted with. That is a new question, and I don't think the answer is obvious in either direction.

29. Lenar Kess 00:12:18

This is also the first time I can point at a named platform cutting off a named agent belonging to a named competitor. We have had rate limits and robots-file disputes for twenty years. This is a popup with a company's name written into it.

30. Damra Vol 00:12:32

And Meta has said nothing, which tells you they're still deciding whether this is a contract fight or a computer-fraud fight. Those go to different lawyers and they end in different places. A contract fight ends in a deal with a revenue share attached. A computer-fraud fight ends in a precedent about whether an agent acting on a user's instruction, with the user's own credentials, counts as authorized access. Everyone building anything that touches a logged-in session is downstream of that answer, including the people who haven't started yet.

31. Lenar Kess 00:13:04

Data Center Watch counted forty-five American data center projects blocked or delayed by local opposition between April and June — sixty-eight billion dollars' worth. They say that's more than half of the large developments in that window. Newley Purnell has it at Bloomberg. That's a research group with a position, so I'd hold the precision loosely, but the direction matches everything else we've seen this year.

32. Damra Vol 00:13:28

Local opposition is the one constraint in this business you can't route around with capital, because what's being purchased is a permit from people who live next to the substation. And the financing changed in the same news cycle. The Financial Times has a piece on residual value guarantees: data center operators are increasingly getting them, with Nvidia and Broadcom backstopping their own customers' purchases.

33. Lenar Kess 00:13:52

Walk me through the mechanics.

34. Damra Vol 00:13:54

A vendor sells you hardware, and then separately underwrites what that hardware will be worth when you're finished with it. That turns a capital purchase into something closer to a lease, it keeps the spend further from the balance sheet, and it lets the operator carry a gentler depreciation assumption. The whole build looks cheaper per year. It also means the vendor now holds the price risk on the secondary market for its own products. If those assets depreciate faster than anyone is modeling, the loss doesn't vanish. It moves onto the balance sheet of the company that manufactured them.

35. Lenar Kess 00:14:27

And Bloomberg reports SoftBank is seeking more than eleven billion dollars in debt for its OpenAI investment. Ten billion of that in dollars, plus a euro tranche. It would be one of the largest junk bond sales ever done.

36. Damra Vol 00:14:40

So there are now three parties holding pieces of the same risk. The operator who signed the lease. The vendor underwriting the resale value of what it sold. And bondholders who bought a high-yield instrument priced on demand holding up. None of that is a problem in any quarter where revenue keeps climbing. It becomes a named problem in the first quarter it doesn't, and all three of them discover it at once.

37. Lenar Kess 00:15:05

Google put out an open agentic orchestrator called AX. Five hundred and twenty-six points on Hacker News with two hundred and twenty-seven comments, which is the largest developer reaction in today's batch. The top comment is the one I'd read first: somebody asking what the converged agent workflow even is at this point, given that everybody is shipping a harness and nobody agrees on what a harness contains.

38. Damra Vol 00:15:29

That comment is an accurate description of the field. We have maybe six competing answers to where the model stops and the scaffold starts, and every vendor's answer happens to match whichever slice of the pipeline that vendor already owns.

39. Lenar Kess 00:15:43

Chris Tate shipped something called Contact Sheets for agent browser sessions. You record an interaction and get timestamped frames of what the agent saw, with the changes between frames highlighted. Pete Hunt quote-posted it, which is how it reached me. Browsing-agent bugs can blink. They appear in one frame, the page re-renders, and the text transcript says everything went fine.

40. Damra Vol 00:16:06

That's the correct instinct for the whole category. A text log is a terrible record of a visual process, and we've been pretending otherwise because text is what we already had a pipe for. It's also cheap to build, which means it either gets absorbed into every harness within three months or it's obsolete within three months. I can't construct a third outcome.

41. Lenar Kess 00:16:27

A paper from Hao Fu, Baiting Zhu, and their colleagues held me longest. They call it EvoPilot, and it's a thirty-seven-day autonomous research campaign run against a live recommender system — the retrieval layer behind a feature called Video Deep Dive, working over an hourly-refreshed index of hundreds of millions of videos. Seven research directions, executed by the agent with humans gating each round.

42. Damra Vol 00:16:52

And the headline results are deliberately modest. A seven-day randomized online evaluation estimated a zero point six six percent relative improvement in one slice of their retention metric. Durable state recovered an interrupted round and saved roughly five GPU-hours. Those numbers aren't why the paper matters.

43. Lenar Kess 00:17:12

Their failure case does more work than either number. An earlier, cruder autoresearch attempt looked at whether an interaction head helped, and attributed a twenty-two percentage point decline in offline hit rate to that head. EvoPilot's verification traced the decline to a pre-existing defect in the evaluation code that was producing output depths of three thousand and six hundred. They repaired it, reran a matched comparison, and got an improvement of three point two zero percentage points. Opposite sign.

44. Damra Vol 00:17:42

So the first run ran to completion, produced a number, and the number was backwards. The paper enumerates four ways that happens: the code change is a no-op, the data windows leak, the evaluator's semantics drift, or the two arms traverse different serving funnels. All four look like a finished experiment from the outside. If you're running any autonomous experiment loop at all, that list is what you check your own harness against this afternoon.

45. Lenar Kess 00:18:09

And DAIR.AI flagged a separate paper on recursive self-improving agent harnesses that names three defects in how harnesses get built, which ties back to where we opened. Klein wants a line drawn at models improving their successors. Here is a documented case of a system improving its own experimental process and very nearly publishing a false conclusion while doing it.

46. Damra Vol 00:18:33

The case for the line and the case against it, inside one paper. The system caught its own error, and the system also produced the error. Whether you find that reassuring depends on whether you believe the next iteration catches the next error, and there's no evidence in the paper either way.

47. Lenar Kess 00:18:50

Let me run the rest. Z.ai released ZCode under Apache 2.0, and they didn't hold anything back. The repo has the desktop app, the web workspace, and the backend in it. It also has the agent command-line tool and the runtime. The announcement came from Z.ai on X about twelve hours ago, and it's the top item on the local-model subreddit this morning. They shipped fixes for the previously reported security issues alongside the license change.

48. Damra Vol 00:19:19

Shipping the remediation with the license is what makes it credible rather than a press release. And open-sourcing a harness is a different move from open-sourcing weights, which I think people undervalue. Weights you can't fork without a cluster. A harness you can fork on a laptop this afternoon, and the harness is where the lock-in has actually been accumulating for the last eighteen months.

49. Lenar Kess 00:19:41

The Information reports DeepSeek's Liang Wenfeng told investors that training on Huawei chips is one of the company's biggest bets, with Huawei set to deliver training silicon in the fourth quarter or early 2027. They've been running inference on Huawei parts for a while already.

50. Damra Vol 00:19:58

Training is a much harder ask than inference, and the gap isn't marketing. You need the collective-communication layer stable for weeks rather than seconds, and you need failures to be recoverable in the middle of a run. Inference is forgiving and embarrassingly parallel. If DeepSeek completes a full frontier training run on domestic silicon, the export-control conversation changes overnight. The window they gave is far enough out that I'd read it as a statement of intent rather than a schedule.

51. Lenar Kess 00:20:27

Alibaba named a senior researcher, Dayiheng Liu, to head the Qwen project after several reorganizations this year. That's Juro Osawa at The Information. And Qwen shipped Qwen-Image-2.1, a seven billion parameter open-weight image model, with native transparency support and up to ten reference images. They claim it beats most closed-source models. Nobody I'd trust has tested that yet.

52. Damra Vol 00:20:54

A native alpha channel is a bigger deal than it sounds for anyone doing composition work, because the alternative is a segmentation pass that eats your edges. And Rest of World has a line about the

Emirates that I keep coming back to — the Emirates owns the machines but rents the intelligence. That's the entire sovereign-compute problem in eight words, and Nvidia's next free model is what might change it.

53. Lenar Kess 00:21:18

On the hobbyist end, somebody ran the full Kimi K3 across a sixteen-box GB10 cluster. That's two point eight trillion parameters. They report thirty tokens per second of coding throughput and a hundred and thirty-six tokens per second at concurrency peak, on a custom runtime they wrote to make it work. All self-reported. And there's a do-it-yourself take on the Jev decision models built with logit manipulation instead of fine-tuning, whose author opens by calling the Jev hype overhyped by a large margin.

54. Damra Vol 00:21:48

[laugh] That's the least oversold release note of the week. And it isn't alone. Jared Palmer's Kev is a small Jev-like family built on top of Qwen3.5, and it hit a hundred and thirty-five points on Hacker News the same night. A continual-learning project called mini-AGI, trained on eight gigabytes of video memory, hit a hundred and eleven. Two reimplementations and a skeptical benchmark within hours of each other, which is what a technique looks like right before it stops being proprietary.

55. Lenar Kess 00:22:19

Last one. Ireland's Data Protection Commission fined Google four hundred and three million euros over how it processed location data, following complaints from European consumer rights groups, and gave the company six months to comply. Olivia Fletcher at Bloomberg.

56. Damra Vol 00:22:36

The six months matters more than the four hundred million. The fine is a line item on a quarterly report. Changing how location data gets collected and retained inside six months is an engineering schedule with a regulator attached to the end of it, and that's what turns up in somebody's sprint planning next week.

57. Lenar Kess 00:22:55

One word in the summit readout decides how much of this morning's first hour was theater, and the word is notification — whether anybody commits to a definition of an incident, or whether a channel gets announced without one and the definition gets written later by whoever is still in the room. [pause] Damra Vol, Lenar Kess.

Hosts on this episode

- Lenar Kess moderator
- Damra Vol critic