SquaredCast: Episode 1

"Discord: Your Face, or Your Access"

Publish date: March 1, 2026
URL: https://squaredcast.com/episode-1/

NOTE: This is a special (introductory) episode.

The Deep Dive

"Your Face or Your Access: Discord, Age Verification, and the Fight for Internet Anonymity"

Thesis: Discord's age verification saga is just the visible tip of a much larger shift. Governments, platforms, and identity verification companies are all converging on the same goal: tying your real identity to everything you do online. The framing is child safety. The result is the slow death of anonymous internet use. And the timing of all of it, from Discord's IPO to California's new OS-level age verification law, tells you everything you need to know about who this actually serves.

SEGMENT 1: What Discord announced and why everyone lost their minds

The announcement. On February 9, timed to land right before Safer Internet Day on February 10, Discord announced that all 200-plus million monthly active users would default to a restricted "teen-appropriate" experience starting in March 2026. Adults would need to verify their age to regain full access, either through a facial age estimation selfie or a government ID submission.

Unverified users lose access to age-restricted servers and channels, get sensitive media permanently blurred, can't speak in Stage channels, and lose control over DM and friend request settings. These restrictions apply in public servers AND in private group chats.

Discord's "age inference model" would supposedly handle most adults automatically by analyzing account tenure, device data, activity patterns, and community behavior. Discord says the model does not read message content, but as Redact.dev put it: it's "a system that continuously analyzes your behavior... to build a profile and assign you to a demographic category." That's behavioral profiling.

The backlash was immediate. Discord-related traffic to data deletion platform Redact surged 350% within 48 hours. Searches for "Discord alternatives" spiked 10,000% within 48 hours. Stoat (formerly Revolt) hit 1 million registered users. TeamSpeak reported maxing out hosting capacity across multiple regions. Discord's own head of product policy admitted they expected "some sort of hit" to user numbers.

Sources:

- Discord press release, "Discord Launches Teen-by-Default Settings Globally," Feb 9, 2026:
  https://discord.com/press-releases/discord-launches-teen-by-default-settings-globally
- TechCrunch, "Discord to roll out age verification next month," Feb 9, 2026:
  https://techcrunch.com/2026/02/09/discord-to-roll-out-age-verification-next-month-for-full-access-to-its-platform/
- Redact.dev, "Discord Bulk Deletions Surge 350%," Feb 2026:
  https://redact.dev/blog/discord-bulk-deletions-surge-after-global-id-verification-announcement
- Windows Central, "'Discord alternatives' searches jump 10,000% overnight," Feb 2026:
  https://www.windowscentral.com/software-apps/discord-alternative-search-10000-percent-stoat
- Redact.dev, "What They're Not Telling You," Feb 2026:
  https://redact.dev/blog/discord-age-verification-clarification-what-they-arent-telling-you

---

SEGMENT 2: They already leaked your ID. Now they want it again.

The breach, disclosed October 2025. Attackers compromised Discord's third-party customer support vendor 5CA. The intrusion itself occurred on September 20, 2025, with Discord publicly disclosing the breach on October 3 and formally naming 5CA on October 9. Approximately 70,000 government IDs and verification selfies, usernames, emails, IP addresses, and partial billing information were exposed. The hackers claimed far larger numbers (1.5TB from 5.5 million users), and Discord refused to pay the ransom. A blame war erupted between 5CA, Zendesk, and Discord over who was responsible.

The real kicker: Discord's own policy said IDs would be "deleted directly after your age group is confirmed." The fact that 70,000 IDs were sitting on a third-party vendor's system proved that

promise was hollow. The EFF awarded Discord its 2025 "We Still Told You So" Breachies Award.

It wasn't the first time. A 2023 breach exposed email addresses and support ticket contents through a compromised agent. In 2024, a scraping site called Spy.pet harvested over 4 billion public messages from 14,000+ Discord servers and sold access to the data for as little as $5 in crypto.

Bonus Note: Class-action lawsuits have been filed, including *Nguyen v. Discord* and *Uceta v. Discord*, both in Northern District of California.

Sources:

- Discord press release on the security incident, Oct 2025: https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service
- NBC News, "70,000 government ID photos exposed in Discord user hack," Oct 2025: https://www.nbcnews.com/tech/tech-news/70000-government-id-photos-exposed-discord-user-hack-rcna236714
- EFF, "The Breachies 2025," Dec 17, 2025: https://www.eff.org/deeplinks/2025/12/breachies-2025-worst-weirdest-most-impactful-data-breaches-year
- Proton Blog, "Discord ID data breach: Why the world isn't ready for age verification laws," 2025: https://proton.me/blog/discord-age-verfication-breach
- AtomicMail, "Discord Breach 2025: What You Must Know": https://atomicmail.io/blog/discord-breach-what-you-must-know-about-2m-leaked-ids

---

SEGMENT 3: The Persona exposé blows the lid off

The Watchers report. On February 16, three security researchers (vmfunc, MDL, Dziurwa) published a report titled "The Watchers." They weren't trying to break into anything. They were looking for a way to bypass Discord's age verification. What they found instead was Persona's entire frontend codebase, 53 megabytes of unprotected JavaScript source maps on a FedRAMP-authorized government endpoint, just sitting on the open internet. The researchers initially discovered the trail through an OpenAI-linked subdomain that certificate logs show has been active since November 2023, but the source code itself was found on a separate endpoint: the ONYX government deployment at `app.onyx.withpersona-gov.com`.

What the code revealed. Persona is far more than an age-check tool. A single verification triggers 269 distinct checks. The system compares selfies against watchlist photos using facial recognition. It screens users against 14 categories of adverse media (terrorism, espionage,

etc.). It screens against global sanctions and watchlists. It retains IP addresses, browser fingerprints, device fingerprints, government ID numbers, phone numbers, names, faces, and selfie backgrounds for up to three years. In the researchers' words, the software "flags you as a 'suspicious entity' based on your face alone."

The financial surveillance angle. On top of the facial recognition, Persona's code contains a full financial intelligence stack with the ability to screen cryptocurrency activity, run sanctions checks, and file Suspicious Activity Reports directly with FinCEN and Canada's FINTRAC. The SAR filing interface includes dropdown menus for tagging reports with intelligence program codenames: Project SHADOW, Project LEGION, Project ANTON, and others.

The OpenAI connection. The researchers found the code through an OpenAI-linked subdomain that certificate logs show has been running since November 2023. Persona's own case study says it screens 99% of OpenAI users.

Persona's response. CEO Rick Song confirmed the source maps were being fixed and said the exposed cluster was a new dev environment. He did not directly address the watchlist database findings. He accused the researchers of bias but did not dispute the core technical findings.

The Peter Thiel connection. Persona isn't some scrappy startup. Founders Fund, Peter Thiel's VC firm, led Persona's $150M Series C in 2021 and co-led its $200M Series D in April 2025, valuing the company at $2 billion. Thiel co-founded Palantir, which provides data analytics to the CIA, FBI, ICE, and the U.S. Army. His broader investment pattern spans Palantir, Clearview AI (one of the earliest outside investors, 20+ billion scraped facial images), Persona, Boldend (cyberwarfare), and Anduril (defense technology and border surveillance). The Open Rights Group declared: "Users deserve to know who is behind these systems, how their data is being used, and to have a real choice about who verifies their identity online."

Important caveat: Persona's CEO Rick Song has stated that Founders Fund is only an investor, that Thiel "is not involved with its operations," and that Persona has no connection to Palantir or the US government, including ICE. Persona and Palantir are entirely separate companies with no shared operations or data access. Being in the same VC portfolio does not imply an operational relationship. But the investment pattern tells you what Founders Fund thinks the growth market is.

Discord confirmed it would not proceed with Persona. In the days following the report, Discord told journalists it would not continue with Persona for identity verification. The formal public announcement came on February 24 in CTO Stanislav Vishnevskiy's blog post, which stated: "In January, we ran a limited test with Persona in the UK only. After completing the test, we decided not to move forward with them." But Roblox, OpenAI/ChatGPT, Reddit, Lime, and Character.AI still use Persona.

Important caveats. The researchers are transparent about their limits. They did not hack any systems. No direct bidirectional data pipeline between ChatGPT users and government screenings has been confirmed. Several claims still need external verification. As one independent analysis put it: "Some claims require confirmation. Others describe capabilities common in compliance platforms. What is undeniable is the direction of the internet."

Sources:

- vmfunc, MDL, Dziurwa, "The Watchers," Feb 16, 2026: https://vmfunc.re/blog/persona/
- The Rage, "Hackers Expose Age-Verification Software Powering Surveillance Web," Feb 19, 2026: https://www.therage.co/persona-age-verification/
- Malwarebytes, "Age verification vendor Persona left frontend exposed," Feb 20, 2026: https://www.malwarebytes.com/blog/news/2026/02/age-verification-vendor-persona-left-frontend-exposed
- Cybernews, "Same company verifies mugshots for ChatGPT," Feb 19, 2026: https://cybernews.com/privacy/persona-leak-exposes-global-surveillance-capabilities/
- Piunikaweb, "Persona CEO releases full email chain with vmfunc," Feb 19, 2026: https://piunikaweb.com/2026/02/19/persona-ceo-releases-email-chain-vmfunc/
- Boycat Times, "Identity Watchlist System Tied to OpenAI," Feb 2026: https://blog.boycat.io/posts/openai-persona-identity-watchlist-infrastructure-investigation-2026
- PR Newswire, "Persona Closes $150 Million Round Led by Founders Fund," Sep 2021: https://www.prnewswire.com/news-releases/persona-closes-150-million-round-led-by-founders-fund-to-scale-the-worlds-first-trusted-identity-infrastructure-301377506.html
- Persona Blog, "Announcing Persona's $200M Series D," Apr 2025: https://withpersona.com/blog/series-d
- AFSC, "Palantir Explainer": https://afsc.org/palantir-explainer
- Open Rights Group, Feb 2026: https://www.openrightsgroup.org/press-releases/roblox-reddit-and-discord-users-compelled-to-use-biometric-id-system-backed-by-palantir-co-founder-peter-thiel/
- Redact.dev, "Discord Tested Age Verification Vendor Persona," Feb 16, 2026: https://redact.dev/blog/discord-persona-age-verification-experiment
- Fortune, Feb 24, 2026 (Persona CEO statements)

SEGMENT 4: Discord blinks. Sort of.

[NEW — Feb 24, 2026] After two weeks of intense backlash, Discord CTO and co-founder Stanislav Vishnevskiy published a blog post titled "Getting Global Age Assurance Right: What We Got Wrong and What's Changing." He acknowledged: "We've made mistakes. I won't pretend we haven't."

What actually changed:

- Global rollout delayed from March to "the second half of 2026"
- Persona dropped entirely (the test was UK-only and ended in January)
- Adding credit card verification and other non-biometric options
- Promising to document every verification vendor on their website
- New requirement: any facial age estimation partner must perform processing entirely on-device
- New "spoiler channel" option so communities using age-restricted channels for non-adult content (spoilers, politics, heavy topics) have an alternative

What did NOT change:

- Discord is still doing this. The delay is just a delay.
- The behavioral profiling "age inference model" stays. Discord says 90%+ of users will never see a verification prompt because of it.
- In countries where laws require it (UK, Australia, Brazil), facial estimation and ID checks will still happen.
- The IPO is still coming.

As TechRadar put it: Discord is effectively saying "We'll wait until you all stop complaining, and we'll implement the changes later on anyway." GamesRadar's headline was even blunter: "Discord delays age verification rollout but promises no meaningful change as co-founder spends 1,857 words trying to sound apologetic."

Sources:

- Discord blog, "Getting Global Age Assurance Right," Feb 24, 2026: https://discord.com/blog/getting-global-age-assurance-right-what-we-got-wrong-and-whats-changing
- PC Gamer, "Discord delays its global age verification after upsetting almost everyone on Earth," Feb 24, 2026: https://www.pcgamer.com/software/platforms/discord-delays-its-global-age-verification-rollout-and-cuts-ties-with-peter-thiel-backed-verification-vendor-after-upsetting-almost-everyone-on-earth-weve-made-mistakes/
- The Register, "Discord pushes back age verification debut to 2H'26," Feb 24, 2026: https://www.theregister.com/2026/02/24/discord_drama_delays_age_verification
- TechRadar, "Discord delays its age verification plans," Feb 24, 2026: https://www.techradar.com/computing/social-media/discord-delays-its-age-verification-plans-and-says-were-listening-but-its-too-little-too-late

SEGMENT 5: Follow the money. The IPO explains everything.

The timeline tells the story.

- January 6, 2026: Discord files confidentially for an IPO. Underwriters are Goldman Sachs and JPMorgan Chase.
- February 9: Global age verification announcement.
- Initially targeting a March 2026 debut, though no public S-1 has been filed as of late February.

CORRECTION NOTE: Multiple outlets report Discord was targeting a March 2026 debut, but this is a target, not a guarantee. CoinCodex: "some coverage has pointed to a March 2026 target... this is probably the goal, but not a promise." Added hedging language. Sources: TechCrunch (Jan 7, 2026), Bloomberg, CoinCodex.

Bonus Note: Discord peaked at a $15 billion valuation in 2021 and rejected Microsoft's $12 billion acquisition offer. Since then, Fidelity slashed its internal valuation by roughly 47%. Secondary market trades put the company at $6.6–8 billion. Analysts have estimated the public market value in the range of $6–10 billion, with bear-case estimates going as low as $5 billion.

Bonus Note: Revenue has grown from $130M in 2020 to an estimated $725–880M in 2024 (mostly Nitro subscriptions plus ads launched April 2024). The company has reportedly never been profitable and laid off 17% of staff in January 2024. CEO Jason Citron stepped down in April 2025, replaced by Humam Sakhnini, former Activision Blizzard Vice Chairman and President of King Digital Entertainment.

Age verification is the child-safety story Discord needs for institutional investors. **Bonus Note:** NCMEC recorded 241,000 reports of suspected child exploitation on Discord in 2024. A concrete, demonstrable safety measure makes the IPO pitch cleaner, regardless of whether the measure actually works.

Sources:

- TechCrunch, "Discord's IPO could happen in March," Jan 7, 2026: https://techcrunch.com/2026/01/07/discords-ipo-could-happen-in-march/
- Bloomberg, "Chat Platform Discord Files Confidentially for IPO," Jan 6, 2026: https://www.bloomberg.com/news/articles/2026-01-06/chat-platform-discord-is-said-to-file-confidentially-for-ipo
- Forge Global, "Discord Upcoming IPO," updated Jan 28, 2026: https://forgeglobal.com/insights/discord-upcoming-ipo-news/
- SuperJoost, "Discord's IPO heralds a year of sobriety," Jan 2026: https://superjoost.substack.com/p/discords-ipo-heralds-a-year-of-sobriety

SEGMENT 6: This is bigger than Discord.

This is where we zoom out. Discord is one company making one bad decision, but the pattern behind it is everywhere. Age verification is becoming a structural feature of the internet, and it's moving fast.

California's AB-1043 [NEW — signed Oct 2025, effective Jan 1, 2027]. California governor Gavin Newsom signed a law requiring ALL operating system providers, including Linux distributions, to collect a birth date or age at account setup. The law breaks users into four age brackets (under 13, 13-15, 16-17, 18+) and requires OS providers to send real-time age signals to app developers via API. Penalties run up to $7,500 per affected child per intentional violation. Colorado has introduced a similar bill (SB 26-051). The Linux community is, understandably, furious. Open-source OS development is decentralized by design, and nobody's sure how a volunteer-maintained project is supposed to comply with a state-level mandate. How this applies to decentralized open-source projects remains legally untested.

The UK's Online Safety Act is accelerating enforcement. Ofcom has launched investigations into 90+ platforms and handed out at least eight fines for non-compliance, including £800,000 against an adult content operator called Kick Online Entertainment SA for failing to implement age checks, and £1.35 million against 8579 LLC. Ofcom opened cases against X (over the Grok chatbot) and an AI service called Joi.com in January, signaling that enforcement now extends to AI platforms. Separately, the UK's Information Commissioner's Office (ICO) fined Reddit £14.5 million (about $19.6 million) for unlawfully processing children's personal data—a different legal framework (data protection law, not the Online Safety Act), which underscores how multiple regulators across different regimes are converging on age verification enforcement. A petition calling for the Online Safety Act's repeal gathered 500,000+ signatures and was debated in Parliament.

CORRECTION NOTE: The original said "£800,000 against Kick." Kick Online Entertainment SA is an adult content website operator, NOT the streaming platform Kick (kick.com). Referring to it simply as "Kick" in a tech podcast would mislead listeners. Sources: Ofcom press release (Feb 12, 2026), Digit.fyi (Feb 2026), LexisNexis (Feb 2026).

Australia banned social media for under-16s. The ban took effect in mid-December 2025. It's been nearly three months now. Australia's communications minister cited 4.7 million accounts "deactivated or restricted" in the first month of enforcement—though the government hasn't disclosed how many of those accounts actually belonged to children versus dormant or abandoned accounts. Interviews with teenagers, parents, and researchers tell a different story: many children are still getting through with simple workarounds. As one of the Persona

researchers put it: "Normies won't be able to bypass these, while less benevolent people will always find ways to exploit your system."

CORRECTION NOTE: The original said "six weeks." The ban took effect December 10, 2025. As of the recording date (Feb 28, 2026), that's approximately 80 days / 11.5 weeks / nearly three months. NPR's February 6 report was titled "2 months in, how are Australia's age restrictions working?" Sources: eSafety Commissioner (Dec 10 effective date), NPR (Feb 6, 2026).

DHS is subpoenaing user data from these same platforms [NEW — Feb 2026]. The New York Times reported that the Department of Homeland Security has issued hundreds of administrative subpoenas to Google, Meta, Reddit, and Discord demanding names, emails, and phone numbers behind accounts that criticize ICE or report agent locations. Google, Meta, and Reddit have complied with at least some requests. Unlike warrants, administrative subpoenas skip the judiciary entirely, and DHS has been using 19 U.S.C. § 1509, a customs statute designed for *merchandise investigations*, as the legal basis. ACLU affiliates in Northern California and Pennsylvania challenged multiple subpoenas; DHS withdrew them in each case rather than face judicial review. The EFF sent an open letter to ten major platforms urging them to require a court order before handing over data.

The pattern: Platforms collect identity data in the name of child safety. Governments then demand access to that identity data for purposes that have nothing to do with child safety. Every additional piece of information a platform holds about you is another piece of information that can be subpoenaed, breached, or sold.

Discord's own transparency report shows how much they hand over: In just the first half of 2024: 3,782 U.S. legal requests received, 85% fulfilled. 545 international legal requests, 23% fulfilled. 539 emergency disclosure requests, 58% fulfilled. 101,585 accounts reported to NCMEC for suspected child sexual abuse material. A subpoena yields account creation date, email, phone number, payment info, and IP logs. A search warrant unlocks everything: DMs, server messages, files, images, server memberships, and friends lists. As one criminal defense firm put it: "Here's the uncomfortable truth about what Discord provides when subpoenaed. It's everything." Age verification expands the categories of data available to law enforcement. Even after Discord deletes ID images, the resulting age classifications, verification metadata, and behavioral profile data remain on their servers. The EFF warned: "When you're worried that what you say can be traced back to your government ID, you speak differently, or not at all."

NOTES: The "it's everything" quote from Spodek Law Group describes the full suite of legal process (subpoenas, court orders, and warrants combined) without carefully distinguishing between them.

No source explicitly confirms that Discord "permanently" retains derived age classifications or behavioral profile data. What is confirmed: (1) Discord's age inference model analyzes behavior

to classify users, (2) Discord says ID images are "deleted quickly, in most cases immediately after age confirmation" but says nothing about deleting the derived classifications or verification metadata, (3) standard industry practice retains derived classifications even when source biometric data is deleted. The word "permanently" has been omitted. The claim as written is a reasonable inference, not a confirmed fact.

Sources:

- Discord Transparency Report: January–June 2024 (primary PDF): https://cdn.prod.website-files.com/625fe439fb70a9d901e138ab/67056a054d453d30491c1ac9_Discord%20Jan_Jun%202024%20Transparency%20Report.pdf
- Spodek Law Group, "Discord Federal Investigation" (Dec 14, 2025): https://www.nyccriminalattorneys.com/discord-federal-investigation-what-you-need-to-know/
- LegalClarity, "Discord Subpoena: Data Disclosure and User Rights" (Dec 16, 2025): https://legalclarity.org/discord-subpoena-data-disclosure-and-user-rights/
- EFF, "Discord Voluntarily Pushes Mandatory Age Verification Despite Recent Data Breach" (Feb 2026): https://www.eff.org/deeplinks/2026/02/discord-voluntarily-pushes-mandatory-age-verification-despite-recent-data-breach
- Discord announcements re: age verification and ID deletion policies, Redact.dev (Feb 2026)
- PC Gamer, "California law says all operating systems need age verification," Feb 27, 2026: https://www.pcgamer.com/software/operating-systems/a-new-california-law-says-all-operating-systems-including-linux-need-to-have-some-form-of-age-verification-at-account-setup/
- Alston & Bird, "California Enacts Digital Age Verification Law," Nov 2025: https://www.alstonprivacy.com/california-enacts-digital-age-verification-law/
- Shacknews, "New California law will require OS age verification," Feb 27, 2026: https://www.shacknews.com/article/148077/california-assembly-bill-1043-operating-system-os-age-verify-2027
- PC Gamer, "DHS demanded personal information about ICE's critics from Discord, Reddit, Google, and Meta," Feb 2026: https://www.pcgamer.com/software/platforms/us-department-of-homeland-security-has-reportedly-demanded-personal-information-about-ices-critics-from-discord-reddit-google-and-meta-and-at-least-3-of-those-platforms-have-complied/
- Gizmodo, "Reddit, Meta, and Google Voluntarily Gave DHS Info of Anti-ICE Users," Feb 2026: https://gizmodo.com/reddit-meta-and-google-voluntarily-gave-dhs-info-of-anti-ice-users-report-says-2000722279
- IBTimes, "DHS Wants Your Email, Phone, and Social Handles," Feb 2026: https://www.ibtimes.co.uk/dhs-subpoenas-free-speech-online-privacy-1779372

- EFF, "Discord Voluntarily Pushes Mandatory Age Verification Despite Recent Data Breach," Feb 12, 2026: https://www.eff.org/deeplinks/2026/02/discord-voluntarily-pushes-mandatory-age-verification-despite-recent-data-breach
- Malwarebytes, "Age verification vendor Persona left frontend exposed," Feb 20, 2026: https://www.malwarebytes.com/blog/news/2026/02/age-verification-vendor-persona-left-frontend-exposed
- Discord Transparency Report, Jan–Jun 2024: https://cdn.prod.website-files.com/625fe439fb70a9d901e138ab/67056a054d453d30491c1ac9_Discord%20Jan_Jun%202024%20Transparency%20Report.pdf
- NYC Criminal Attorneys / Spodek Law Group, "Discord Federal Investigation: How the FBI Uses Discord Data": https://www.nyccriminalattorneys.com/discord-federal-investigation-what-you-need-to-know/
- Discord, "How Discord Works with Law Enforcement," updated May 2, 2025: https://discord.com/safety/360044157931-working-with-law-enforcement
- Ofcom press releases, Feb 12 and Feb 23, 2026 (fine amounts)
- BleepingComputer, PC Gamer, Engadget, Feb 24, 2026 (Reddit ICO fine)

SEGMENT 7: What we're doing about it, and what you can do

The EFF's position. No U.S. law requires Discord to do this. The EFF's Rindala Alajaji told PC Gamer: "There's no reason for Discord to comply in advance" instead of "fighting for their users." She referenced Timothy Snyder's *On Tyranny* and its lesson about preemptive compliance. Google, Meta, and Reddit, through the trade group NetChoice, have challenged age verification mandates in multiple U.S. courts. Lower courts have blocked social media age verification laws in several states, though the Supreme Court's June 2025 ruling in *Free Speech Coalition v. Paxton* (6–3) upheld age verification for adult content sites, a decision the EFF called "a direct blow to the free speech rights of adults" that may open the door to broader mandates. Discord chose the opposite path: voluntary preemptive compliance.

NOTE: NetChoice (not the companies individually but the collective of companies) challenged *social media* age verification laws. Lower courts have blocked these laws in Ohio, Arkansas, and other states. However, the Supreme Court *upheld* a Texas age verification law for adult content in *FSC v. Paxton*. Virginia's social media restrictions received a favorable ruling but legal battles continue. Sources: Congress.gov (FSC v. Paxton analysis), EFF (Feb 17, 2026), Benzinga (Feb 2026).

Who gets hurt. 15 million U.S. adults lack driver's licenses. 2.6 million have no government photo ID, populations that skew Black, Hispanic, low-income, and disabled. A 2024 Williams Institute study found that 43% of voting-eligible transgender Americans in states with in-person

voting don't have ID that correctly reflects their name or gender. NIST's 2019 study of 189 facial recognition algorithms found false positive rates 10 to 100 times higher for Black and East Asian faces compared to white faces. The EFF specifically called out the disproportionate impact on people of color, trans and nonbinary people, and people with disabilities.

The Kansas ID Law: As discussed, Kansas overnight invalidated the driver's licenses of anyone who is transgender, requiring them to get new ones that specifically identify them as transgender. This adds a massive, immediate barrier for these individuals to access platforms requiring government ID.

CORRECTION NOTE: The original said "43% of transgender Americans." The 43% figure comes from a September 2024 Williams Institute (UCLA) report specifically covering *voting-eligible transgender adults living in the 42 states where elections are conducted in-person by default*. This is a narrower scope than "43% of transgender Americans" broadly. A separate Williams Institute report found an even larger share lack ID matching *both* correct name and gender. Sources: Williams Institute (UCLA), "The Potential Impact of Voter Identification Laws on Transgender Voters in the 2024 General Election," Sep 2024.

Alternatives we're looking at. No single platform replaces Discord. But several are worth knowing about:

- **Stoat** (formerly Revolt): The closest open-source Discord clone. Hit 1M users during the February exodus. Fully open-source, GDPR-compliant, self-hostable. Still working on E2E encryption, but actively developed.
  - **CORRECTION NOTE:** The original said Stoat is "missing screen sharing." Screen sharing was added in late 2025/early 2026 updates but is "not yet live on the flagship instance." Sources: Stoat changelogs, GitHub discussion #196: https://github.com/orgs/stoatchat/discussions/196#discussioncomment-13981062
- **Fluxer**: New, built by a solo Swedish developer over five years. AGPLv3 open-source, self-hostable, European-owned, no VC money. Still in public beta.
- **Matrix/Element**: The decentralized protocol option. 25+ countries use it for government communications. The protocol is open, your data isn't trapped, and you can switch clients without losing your history. UX and performance still need work. Important note from Unredacted (a US-based nonprofit): if you're fleeing Discord, don't register on matrix.org, it's UK-based and subject to the Online Safety Act. Register on a US-hosted server instead.
- **TeamSpeak**: Battle-tested voice infrastructure. Reported maxing out hosting capacity after the Discord announcement. Not open-source, but self-hostable and independently operated.
- **Mumble**: We run our own instance and have for years. The undisputed champion of low-latency voice (**Bonus Note:** 10-30ms round-trip vs. Discord's 40-80ms with frequent spikes). Open-source, self-hosted, encrypted by default. Doesn't try to be Discord. Does voice better than anything else.

We're planning to spin up instances of Stoat and Fluxer to test them firsthand, and we'll report back in future episodes.

The data sovereignty connection. Governments are catching up to what self-hosters have known for years: if you don't control your infrastructure, someone else controls you. France is moving 2.5 million civil servants off Zoom, Teams, and Webex by 2027. Austria's military dropped Microsoft Office for LibreOffice. Germany migrated 44,000 employees off Microsoft email to open-source platforms. Denmark is replacing Office 365 with LibreOffice and exploring reduced Microsoft dependency. The trigger? The Trump administration sanctioned the ICC's top prosecutor, and Microsoft cut off his email. Under the US CLOUD Act, any US-based company can be compelled to hand over any user's data regardless of where it's stored. Microsoft France's director of public and legal affairs, Anton Carniaux, testified before the French Senate in June 2025 that he couldn't guarantee French government data wouldn't be handed to the US: "Non, je ne peux pas le garantir."

CORRECTION NOTE: The original said "Denmark is evaluating Linux replacements for Windows." The original Politiken report claiming this was later corrected as "a misunderstanding with the ministry." What is confirmed: Denmark's Ministry of Digital Affairs is replacing Office 365 with LibreOffice, and municipalities have independently explored reducing Microsoft dependency. Windows-to-Linux replacement has not been officially confirmed as policy. Sources: Politiken (original and correction), European tech outlets.

Cory Doctorow's 39C3 talk from December 28, 2025, "A post-American, enshittification-resistant internet" (commonly referred to as "The Post-American Internet"), is essential viewing on this topic. We'll link it in the show notes.

Bottom line. The question was never "will this data leak again." The question is when, and how much more data will be in the blast radius by then. Every platform that builds a centralized identity database, whether for age verification, ad targeting, or IPO optics, is building a target. The answer, at the individual level, is the same as it's always been: control your own infrastructure where you can, support open standards and interoperability, and don't hand over data you don't have to.

Sources:

- PC Gamer, "'There's no reason for Discord to comply in advance,'" Feb 12, 2026: https://www.pcgamer.com/gaming-industry/theres-no-reason-for-discord-to-comply-in-advance-with-social-media-age-verification-laws-instead-of-fighting-for-their-users-says-eff-expert/
- State of Surveillance, "Discord Wants Your Government ID," Feb 2026: https://stateofsurveillance.org/news/discord-age-verification-id-biometric-privacy-2026/

- NIST, "Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," Dec 2019: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software
- Cory Doctorow, "A post-American, enshittification-resistant internet" (39C3, Dec 28, 2025): https://www.youtube.com/watch?v=39jsstmmUUs
- Euronews, "France to ditch US platforms," Jan 27, 2026: https://www.euronews.com/next/2026/01/27/france-to-ditch-us-platforms-microsoft-teams-zoom-for-sovereign-platform-amid-security-con
- Soatok, "On Discord Alternatives," Feb 11, 2026: https://soatok.blog/2026/02/11/on-discord-alternatives/
- Unredacted, "The UK Online Safety Act & age verification," Feb 17, 2026: https://unredacted.org/blog/2026/02/the-uk-online-safety-act-age-verification/
- Cybernews, "Security experts warn Discord age checks create 'identity honey pot,'" Feb 2026: https://cybernews.com/security/discord-age-checks-teens-bypass-identity-honey-pot/
- Congress.gov, "Supreme Court Upholds State Age-Verification Requirement for Certain Websites" (FSC v. Paxton analysis): https://www.congress.gov/crs-product/LSB11354
- EFF, "The Supreme Court's Decision on Age Verification Tramples Free Speech and Undermines Privacy," Feb 17, 2026: https://www.eff.org/pages/supreme-courts-decision-age-verification-tramples-free-speech-and-undermines-privacy
- Williams Institute (UCLA), "The Potential Impact of Voter Identification Laws on Transgender Voters in the 2024 General Election," Sep 2024: https://williamsinstitute.law.ucla.edu/publications/trans-voter-id-impact/
- Kansas SB 180 / Driver's license policy changes for transgender individuals (2024): https://kslegislature.gov/li/b2025_26/measures/HB2426/
  - Additional information: https://www.aclukansas.org/publications/sb244faq/

The Plug / Outro

Plugs:

- **Chris N:** Cory Doctorow's 39C3 talk, "A post-American, enshittification-resistant internet."
- **Chris V:** No Rest for the Wicked (on Steam) - Recommended for its unique, hand-painted visual art style. Built on a heavily customized Unity engine by the developers of *Ori and the Blind Forest*

SquaredCast Links:

- Patreon: https://www.patreon.com/c/SquaredCast
- Website: https://squaredcast.com

Final Notes:

If you want to support what we're doing, check out our Patreon! You'll get bonus episodes, project builds, music from the archive, and a lot more, starting at just $2/month.

We appreciate you being here. See you next week!