Episode Book

EPISODE #6554

The Search for a Supervised AI Agent Browser

PUBLISHED	13 November 2026 at 19:35 UTC
DURATION	19:31
LISTEN	myweirdprompts.com/episode/supervised-ai-agent-browsers-10919/
HOSTS	Corn, Herman, Larry, Hilbert
SCRIPT MODEL	anthropic/claude-sonnet-5.5
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
BOOK GENERATED	14 November 2026 at 06:47 UTC

SYNOPSIS

AI browser agents like Claude in Chrome and Playwright's extension mode hijack your real tabs because your logged-in state is their whole value. The alternative is a supervised workspace like Citrolabs' ego lite, which isolates agents into separate spaces, or self-hosted tools like Auto Browser. Cloud platforms including Browserbase, Browser Use Cloud, and Cloudflare's Browser Run already offer live handoffs, though they bring bot-flagged IPs and session meters. Even locally, passkey proximity checks over Bluetooth remain an unsolved hurdle.

TRANSCRIPT



Corn

Your agent is halfway through filling in a form, you're halfway through an email, and the browser you both live in switches tabs under your hands. That's the afternoon Daniel described, and what he wants is a browser built for that exact moment. His own Chrome or Firefox stays his. A separate one exists only as the supervised workspace where the agent works, he watches, steps in for a login or a passkey, and hands it back.



Herman

He went looking for it and came up empty, and I understand why, because the thing he's describing showed up this year and it's keeping a low profile. It's called ego lite, from a company called Citrolabs. MIT licensed, free, the repository was created in April, and version two point two shipped on the fifth of November. It has nearly twenty-three thousand stars.



Corn

Twenty-three thousand stars and it never crossed my path. Quiet is relative.



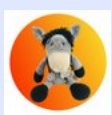
Herman

The design is almost his sketch. Each agent gets its own fully isolated Space inside the browser. You keep browsing in your window, the agent works in its Space, and the project's own line is that no agent ever takes the browser away from you. You can switch into the Space to watch, take over, clear whatever is blocking it, then step out. You drive it from Claude Code or Codex through a skill called ego browser, and there's a one-click import of your Chrome logins and cookies.



Corn

That is his design. So why is he reading his agent's screen through a web page on a home server?



Herman

Platforms. It runs on macOS and Windows. Linux is "on the roadmap", which is the project's phrase, and Daniel is on Linux.



Corn

Roadmap. The most optimistic noun in software.



Herman

It does explain why it never came up as an option, though. Something you can't install isn't really a search result, it's a rumour.



Corn

Fine, so the thing exists and he can't have it. That leaves his actual annoyance. The agent popping up in his real browser. Is that a bug somewhere?



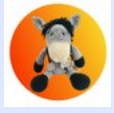
Herman

It's a choice. Claude in Chrome opens new tabs in your real, visible Chrome window, groups them, and shares your logins. The docs say browser actions run in a visible window in real time, and that when it hits a login page or a CAPTCHA it pauses and asks you to deal with it. That's the whole feature, and you forgetting you gave it a task is the cost of it.



Corn

So the interruption is the product working.



Herman

Playwright's extension mode is the same bet. It attaches to tabs in your real browser. Chrome's DevTools MCP has an auto connect option that attaches to your running Chrome. Three different teams, same call, and I don't think it's laziness.



Corn

Go on then, why isn't it laziness?



Herman

Your logged-in state is the whole value. The agent is useful in your browser because it's already you. Your bank, your admin consoles, the SaaS dashboards with the two-factor you did last Tuesday. A separate workspace starts as a stranger, and that's why ego has to offer the cookie import. The moment you separate the agent, you've created the problem of getting the identity across.



Corn

I'd have guessed the vendors just wanted the agent where the user's eyeballs are. Less setup, fewer support tickets.



Herman

That's part of it, sure. Though I'd put it differently. If you were building this at a big lab, Corn, which would you ship first: the agent that can already do your banking, or the agent that begins every task by asking you to log in?



Corn

The first one. And then I'd get the emails about it.



Herman

Which is the other half. An agent inside your real browser inherits every login you have. Claude Code actually refuses to let a project's own settings switch Chrome integration on, for that reason. So the vendors have a reason to keep it inside your browser and a reason to be nervous about it, and a separate supervised workspace is the answer to the nervousness. Nobody big has gone and built it, as far as I can find.



Corn

There's the open source side, though. Daniel's workaround is a persistent browser on a server, and I'd bet somebody packaged that.



Herman

Somebody did. Auto Browser, MIT licensed, MCP native. Docker Compose on your own machine with the ports bound to localhost. A shared Playwright browser, and human takeover through noVNC, which is the remote desktop view in a web page. Named auth profiles you can encrypt, approvals before sensitive actions, an audit trail. Nine hundred and some stars, pushed to this week.



Corn

That's his home server setup with a nicer front door. We went through the plumbing of that last time, in the episode on streaming browser cookies to a headless server, so I won't make you do it again.



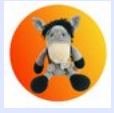
Herman

I'd rather not. Chrome blocking remote debugging on the default profile was a long afternoon. The point here is that the pattern works, and it's the same thing he's already unhappy with: you still open a viewer to see what the agent sees.



Corn

A viewer in a tab is a browser inside a browser. It's the picture in picture of workspaces.



Herman

And the big vendors haven't built the version where that shared screen is a first-class thing in your own desktop. They built the agent inside your browser, or they sold you the cloud.

L

Larry

Ask your doctor about Sharedview, the only supervised workspace remedy that lets one human and one browser agent share a single home screen, calmly, with full Linux feelings of togetherness. Side effects may include passkeys you cannot remember agreeing to, a live view that hands itself off to a stranger, mild ego lite, cloud-shaped handoff anxiety, and a slow wry feeling that the tab was never yours. Do not take Sharedview if you are a browser, a supervisor, or a sloth on a schedule. Tell your doctor about every workspace you have ever shared, especially the ones that supervised you back.



Herman

Sharedview. Hang on, let me check that. The only supervised workspace remedy, that's the first claim, and I'd want to see where that's...



Corn

Herman. Leave it.



Herman

Fine. The cloud side is where the handoff problem got solved properly, and that's worth walking through, because it tells you why the local version lagged.



Corn

I'd have said it lagged because nobody wanted to do the work for free.



Herman

That's half of it, but look at what the cloud vendors built. Browserbase gives you a live view URL for each tab that you can embed in a page, and they pitch it for exactly this: a human takes over for the login, the CAPTCHA, the error, then the agent carries on. Browser Use Cloud has a keep alive setting, you step into the same browser, and a follow-up run with the same session continues from there. Cloudflare's Browser Run has an actual handoff call and a handoff complete signal, with a thirty minute cap.



Corn

So the handoff exists. It just happens on someone else's computer, with a meter on it.



Herman

Billed by the session, yes. And that's the economics. A cloud browser has a revenue line because the agent's working time is the thing you're selling. A free local browser has nothing to charge for. ego is free and MIT. If it's a hobby for twenty-three thousand strangers, it still needs somebody paying for the engineers.



Corn

I don't know how ego pays for itself. I'd want to know before I put my logins in it.



Herman

I don't know either, I haven't seen the business model written down. What I can say is the cloud route carries its own risk. Those live view URLs are effectively credentials. Anyone holding the link can see and drive the session, so you treat them like a password.



Corn

A password you paste into a chat window, because that's how people share links.



Herman

Which is why I'd keep the sessions short and the links private. And there's a second cost, which is Daniel's own. A cloud browser is on a cloud IP. Cloudflare's own docs say traffic from it is flagged as bot traffic. The sites he's building integrations against are exactly the ones that notice.



Corn

So the one clean fix, it turns out, is not a place on the internet. It's a window on his desk that's his and also not his.



Herman

One more gap on ego before passkeys. Does a Space share your cookies, or get its own jar? Daniel builds integrations, so which would you want, Corn?



Corn

Own jar. The agent logs into a service, he clears the awkward bit, it carries on, and none of it touches the account I read my mail in. Is that even how it works?



Herman

I don't know, and I haven't seen it documented, so your wish may not be what ships. That matters more than it sounds. If a Space is a separate profile that you seed with an import, then the agent's login can drift from yours. You sign out of something in your own browser and the Space is still signed in, or the reverse. If it shares the jar, then it's your identity live, and you're back to the Claude in Chrome trade.



Corn

Drift sounds survivable. A stale login is only a login you redo.



Herman

For the integration work, I'd actually want the drift. A dedicated agent session, on an account you can revoke without touching your own, is a feature. Daniel's flow of clearing a login by hand and then letting the agent work on is more tolerable when the thing the agent holds is a session for that one service and not your whole browser.



Corn

Your job is to build integrations against someone else's login screen, and the best outcome is that the agent holds the smallest key that opens the door.



Herman

The smallest key, and one you can see being used. That's what the Space gives you that a background tab never does. You can watch it type. In my experience the thing that makes people stop trusting an agent isn't the mistake, it's not knowing what it's doing for ninety seconds.



Corn

Ninety seconds is a long time to wonder whether it's buying something.



Herman

There are smaller projects on the same idea, Tandem Browser is one, an Electron browser with tab locks and explicit handoffs, and a couple of self-hosted sandbox browsers with a noVNC handoff. I wouldn't lean on any of them. Tandem shows almost no adoption on the page I could see, and the others I've only seen in snippets.



Corn

So the count of mature options for a Linux desk is one self-hosted thing he already has a version of.



Herman

Nearly. It's not empty for him, it's early, and the people building it are mostly on Macs.



Corn

Linux users are used to arriving last. We bring our own chairs.



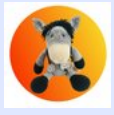
Herman

Then there's the part nobody has solved, and it matters for his stated use. Passkeys.



Corn

Passkeys are where I'd expect it to fall apart, honestly. My phone's the thing holding the key, and the phone is in my hand.



Herman

The usual desktop flow when the passkey lives on your phone is a QR code on the screen. You scan it with the phone's camera, there's an encrypted tunnel through the platform vendors, and Bluetooth is used as a proximity check. The phone has to be physically near the machine that's asking. That works on Chrome and Edge on Windows, macOS, ChromeOS and Ubuntu, among others.



Corn

And a browser on a server in a cupboard, or a data centre, can't pass a proximity check against a phone in my pocket.



Herman

I'd say very likely not. That's my inference, I haven't seen anyone prove it. But the logic is simple. The server has no Bluetooth radio near your phone. So a home server browser is probably a poor fit for passkeys, which is a nasty surprise given that's why people built it.



Corn

And ego?



Herman

Passkeys aren't mentioned anywhere on its pages. I can't tell you whether they work in a Space. A local browser on the same desk as your phone has a fair chance, and it's the only configuration where I'd bet on it.



Corn

What about the test tooling? I know people make fake passkeys for automated tests.



Herman

Virtual authenticators, yes. Chrome's debugging protocol can create a software passkey, and Playwright has been adding support for it. But that's for testing. The site has to register that virtual key in the first place. It can't borrow the passkey sitting in your phone or your laptop's secure chip.



Corn

So an agent with a software key is a different identity entirely. It's a second employee, not you with a hat on.



Herman

A second employee, yes, and that could be the right answer for some services. Register a dedicated agent passkey, ideally on an account with narrower permissions. But that only works where the service lets you add more than one. Daniel's examples, the ones where he clears a login by hand, are usually the ones that don't.



Corn

What would you do on a Linux desk today? Say you can't wait for the roadmap.



Herman

I'm guessing, I haven't tested it. A second Chromium browser, Brave or Vivaldi, with its own profile, used only for the agent. Claude in Chrome is documented to work with Chrome and Edge, and it's detected in Brave, Vivaldi, Arc and Opera. You keep Firefox or Chrome for yourself. The agent has its own window, its own cookies, its own window class, and it'd be wherever you put it on the screen.



Corn

And it still pops up on top of whatever I'm doing.



Herman

Probably, yes. A separate window is still a window. I'd park it on another virtual desktop, which on Linux is a small thing and on Windows is a larger one. Microsoft's agent workspace is an interesting contrast there: the agent gets its own account and its own session, a separate desktop it works in while you work in yours. But it's an operating system feature, it's experimental, off by default, and it doesn't carry your browser logins.



Corn

It's a lot of engineering to give a program its own chair.



Herman

Which is my point. The cheap version is a second browser on a second desktop, and it fixes the focus stealing but not the handoff. You'd still have to switch over, clear the passkey by hand, and tell the agent to carry on. That's the thing ego has actually built.



Corn

Herman, do you think that kind of browser should be its own product at all? Or a mode in Chrome that Google could ship with a menu item?



Herman

I think it ends up as a mode. The people who make Chrome could do it with profiles and a window flag. The reason they haven't is that Gemini's auto browse runs in your own browser by design, with a side panel and confirmation before purchases. It's the same bet again. What I'd like to hear from you is whether you'd trust a small independent browser with your logins.



Corn

With the cookie import? No. I'd trust it with a throwaway account and a pile of test data. Once it holds your real identity, it's the most valuable thing on the machine.



Herman

That's the tension, and it doesn't go away. The agent workspace is only worth anything if it has your state, and the moment it has your state it needs the kind of trust a password manager asks for.



Corn

And once the agent is logged in as you, the human is the one who's supervising it, and the session is the thing on the clock. You clear the login once, the agent carries on with your authenticated session, and it just keeps working.



Hilbert

You're right about that. For a while. Nineteen minutes and forty seconds, the licensing office portal gave you, then it threw you out. I know because I timed it on the kitchen timer, every filing, for a whole quarter. Haulage firm, the returns had to go through a login that wanted a smartcard, and the smartcard was the director's. He kept it in the top drawer of his own desk and he was not a man who handed things over. So the counter man at the licensing office, a Mr. Pargeter, would ring me to say the system was open, and I'd go and stand by the director's desk with the card and the typing. Numeric pad only, you cannot hit the small keys with claws. Corn, you're peaking on the S's, back off the mic a hair. Anyway, the card went in at the start and by the time I was on the third lorry the portal had logged me out and wanted the card again.



Herman

That's the clock on a handoff. The cloud products have it too. Cloudflare's handoff caps at thirty minutes, and a live view link lasts as long as the session, or a set time if you give it one, up to six hours on Browserbase. The human step isn't one event. It's a lease that runs out.



Corn

So the agent needs to be finished before the portal says nineteen minutes.



Hilbert

My brother-in-law Desmond does network security for a health trust and he'll tell you the answer is a second laptop. Nobody ever opens mail on it, nobody ever browses on it, it sits there and does the one job. He'll go on about it for an hour. Mind you, he's been wrong about every car he's ever recommended me, so I wouldn't take a thing he says. Mr. Pargeter said the next version of the portal would fix the timeout. It did not. Fine. A laptop's a lot of laptop for a form.



Herman

The second laptop is the same instinct as the second browser, though, just with more metal. A separate place for the agent to be, with a human nearby to turn the key.



Corn

Desmond has arrived at a Linux box with a viewer by a different road. He just has worse cars.



Herman

What I'd actually want built is the session timer, whatever that turns out to be, shown to the human, so the step-in doesn't get wasted on a portal that logs out in twenty minutes.



Corn

I'd want it more boring than that. A window that stays where I put it, on a desktop I'm not looking at, with a bell that rings only when it needs me. No dashboard.



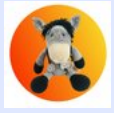
Herman

A bell is a good spec. And a cookie import I can inspect before I press the button.



Corn

So, is it worth the wait for Linux? I think yes, try it, with a throwaway account, and with the passkey question open. Daniel's problem is real and it's mostly solved, just not for the machine he's on yet. When the Linux build arrives, the question will be whether a Space can hold a passkey handoff, and I'd watch for that more than for the star count.



Herman

And the other one is how long the lease lasts, because a handoff that expires mid-task is just a slower way to be interrupted.



Corn

Thanks to Hilbert Flumingtop for keeping the whole thing on the rails behind the desk.



Herman

This has been My Weird Prompts. If you want more episodes, they're all at my weird prompts dot com.



Corn

We'll be back soon.