not.bot

The internet has a bot problem, and it's worse than most people realize. AI can now pass CAPTCHAs, imitate writing styles, generate convincing faces, clone voices, and operate social media personas at industrial scale. Nobody can tell, with any confidence, whether they're interacting with a human or a machine. And the obvious fix, requiring people to verify their real identity, trades one problem for another. You shouldn't have to hand over your government ID just to post a comment or make a bet online.

Not.bot solves this. It lets you prove specific things about yourself with mathematical certainty, without revealing who you are.

Sites that use not.bot get something valuable too: they never collect the data in the first place. Data you don't have isn't a liability because it can't be leaked or hacked. And customers will appreciate knowing that their data can't be sold.

Is this a human?

The most basic question a website can ask is whether it's talking to a real person. Not.bot answers that question with cryptographic certainty. A valid not.bot verification cannot be produced by a bot, a script, or an agent, regardless of how sophisticated. It requires an enrolled human, on their own device, actively participating. That's it. No name, no address, no government ID handed to the site. Just proof that it is a human.

Age verification

Selling alcohol online. Restricting adult content. Complying with regulations that require age checks. These are real business requirements, and the current solutions are either ineffective (self-reported age) or invasive (uploading a government ID to a website you may not trust).

Not.bot lets users prove they're over 18, or over 21, or within a specific age range, without the site ever learning their actual birthdate or anything else about the

user. A cryptographic credential attests to the age fact. The site verifies it and learns exactly what it needs to know: yes or no. Nothing else.

One person, one account

The internet is rapidly collapsing as a forum for discussion because AI has made it so much easier for one person to create dozens or hundreds of fake accounts. The impact is enormous. Misinformation campaigns on social media. Poll manipulation. Advertising disguised as social consensus. Promo abuse. Account sharing that deprives sites of subscription revenue they've earned. Distorted user metrics.

Not.bot can stop this too. Users who choose to can consent to a site pass, a cryptographic token that lets a site recognize them as the same individual across visits, regardless of which alias they use. If someone tries to create a second account, the site catches it. Each site pass is unique to one person and one site. Sites can't use them to track users across the web, even if they buy data from other sites.

Signing content

Beyond verification, not.bot lets people sign what they create. A post, a document, a photograph, a video. Just like an ink signature on paper, a not.bot signature attests that a specific person put their name to something. Unlike an ink signature, it's cryptographically bound to the person.

This matters more every day. AI-generated content is now indistinguishable from human-generated content at scale. Deepfakes are cheap to produce. AI can't fake these signatures, no matter how capable, because producing a valid signature requires the participation of an enrolled human with their own device.

How it works

When you enroll in not.bot, you scan your passport. Julia Social, the company behind not.bot, never sees your passport data. Instead, the data goes to an independent data escrow service, where it is only stored in encrypted form. The escrow service doesn’t have the decryption key. Julia Social has the decryption key but not the data. Neither company can access your data. After enrollment completes, the only accessible copy of your data is on your device.

What Julia Social does get is a cryptographic proof that you're a unique real person with a real passport. That's enough to create a digital identity controlled entirely by your own device.

From that identity, you can create aliases: separate identities for different contexts. Your professional alias. Your activist alias. A throwaway for a forum you visit occasionally. Each alias is cryptographically independent. Nobody can connect your aliases to each other just by examining them.

What makes this different

Most companies that ask for your identity information expect you to trust they will keep it safe. Julia Social has created not.bot in a way that trust isn't necessary. Julia Social doesn't ever have access to your identity information. It doesn't know what aliases you have. It can't read your signatures. It can't tell which sites you visit. Julia Social can't access data it doesn't have.

US law enforcement can identify the person behind a specific signature by presenting a valid legal demand. That process requires both Julia Social and the escrow company to cooperate, takes roughly two weeks, can't be expedited, and works one signature at a time. Bulk surveillance using not.bot is impossible by design.

The full technical specifications are in the *not.bot Privacy and Security Whitepaper*, available for AI-assisted review.

You can verify the authenticity of this document by scanning the signature below:

not.bøt