Privacy is Marketing. Anonymity is Architecture.

Matteo M. December 20, 2025 42,393 views

> *Every company says they "care about your privacy." It's in every privacy policy, every marketing page, every investor deck. But if I can reset your password via email, I know who you are. If I log your IP, I know where you are. If I require phone verification, I have leverage over you.*
>
> ***That's not privacy. That's performance art.***

In 2025, "privacy" has become the most abused word in tech. It's slapped on products that require government IDs, services that log everything, and platforms that couldn't protect user data if they tried.

Real anonymity isn't a marketing claim. It's an architectural decision that makes it *impossible* to compromise users, even if you wanted to. Even if someone put a gun to your head. Even if a three-letter agency showed up with a warrant.

Let me show you the difference.

The Privacy Theater Playbook

Here's how the average "privacy-focused" service actually works:

```
User Journey:
1. Enter email address
2. Verify email (now we have your email)
3. Create password (now we can reset it via email)
4. Add phone for "security" (now we have your phone)
5. Confirm identity for "fraud prevention" (now we have your ID)
6. Enable 2FA (more identity vectors)

Privacy Policy:
"We care deeply about your privacy and only collect
necessary information to provide our services..."

Translation:
We have everything. We log everything.
We just promise to be careful with it.
```

The problem isn't malice. Most services genuinely try to protect user data. But protection implies possession. And possession is the vulnerability.

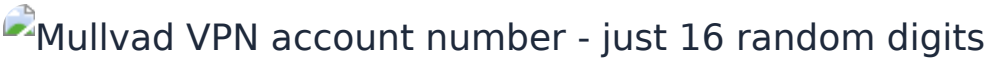
You can't leak what you don't have. You can't be forced to hand over what doesn't exist.

The Mullvad Moment

In 2023, Swedish police raided Mullvad VPN's offices with a search warrant. They wanted user data. Customer information. Connection logs. Anything.

They left empty-handed.

Not because Mullvad refused to cooperate. Not because they hid the data. But because *there was no data to give*. Mullvad's entire identity system is a randomly generated account number. No email. No name. No records.


Mullvad VPN account number - just 16 random digits

Mullvad's entire authentication system: 16 random digits. That's it. That's the whole identity.
When the police realized this, they couldn't even argue. The architecture made compliance impossible. Not difficult. **Impossible**.

That's what real anonymity looks like.

How We Built The Same Thing

When we designed Servury, we asked ourselves: what's the minimum information needed to run a cloud hosting platform?

Turns out, not much:

```
 // What we DON'T collect:
- Email address (no recovery, no marketing, no leaks)
- Name (we don't care who you are)
- IP addresses (not logged, not stored, not tracked)
- Payment information (handled by processors, not us)
- Usage patterns (no analytics, no telemetry, nothing)
- Device fingerprints (your browser, your business)
- Geographic data (beyond what's needed for server selection)

// What we DO store:
- 32-character credential (random alphanumeric string)
```

```
- Account balance (need to know if you can deploy)
- Active services (servers and proxies you're running)

That's it. Three data points.
```

No "forgot password" link. No email verification. No phone number for "account security." Because every one of those features requires storing identity, and identity is the attack surface.

The Trade-Off Nobody Talks About

Here's the part where other "privacy" companies quietly change the subject: **lose your credential, you're done.**

No recovery process. No support ticket that can restore access. No "verify your identity" workflow. If that 32-character string disappears, so does your account.

And you know what? That's *exactly the point*.

> Traditional service: "We can help you recover your account by verifying your identity"
> **Translation:** We know who you are, and we can prove it.
>
> Servury: "We literally cannot help you recover your account"
> **Translation:** We have no idea who you are, and that's by design.

The inconvenience of memorizing (or securely storing) a random string is the *cost* of anonymity. Anyone who tells you that you can have both perfect anonymity AND easy account recovery is lying or doesn't understand the threat model.

What This Actually Means In Practice

Let's walk through a real scenario:

> "*Hi Servury support, I lost access to my account. Can you help me recover it?*"
>
> "*I'm sorry, but we have no way to verify account ownership. If you don't have your credential, the account is inaccessible to everyone, including us.*"
>
> "*But I can prove it's me! Here's my payment receipt, my IP address, the exact time I signed up—*"
>
> "*We don't store any of that information. There's nothing to match against.*"

Is this frustrating for users who lose their credentials? Absolutely. Is it a feature? **Absolutely.**

Because on the flip side:

- Law enforcement can't social engineer your account access
- Hackers can't phish or reset your credentials via email
- We can't accidentally leak your personal information (because we don't have it)
- No government can force us to reveal who you are (because we genuinely don't know)

The Email Trap

Email addresses are the original sin of modern internet identity. They seem harmless. Universal. Convenient. And they completely destroy anonymity.

```
Why email kills anonymity:


1. Email IS identity
```

```
   - Tied to phone numbers
   - Tied to payment methods
   - Tied to other services
   - Recovery mechanisms expose you

2. Email IS trackable
   - Read receipts
   - Link tracking
   - Metadata analysis
   - Cross-service correlation

3. Email IS persistent
   - Exists beyond single service
   - Archived forever
   - Subpoenaed retroactively
   - Leaked in breaches

4. Email IS social engineering
   - Phishing vector
   - Password reset vulnerability
   - Support ticket exploitation
   - Impersonation risk
```

The moment you require an email address, you're not building for anonymity. You're building for accountability. And sometimes that's fine! Banks should know who you are. Government services should verify identity. But cloud infrastructure? VPNs? Proxy services?

We shouldn't need to know a damn thing about you.

Crypto Payments: Not Just For Criminals

We accept cryptocurrency not because we're trying to hide from authorities. We accept it because traditional payment systems are surveillance infrastructure.

Every credit card transaction creates a permanent record linking your identity to your purchase. Your bank knows. The payment processor knows. The merchant knows. And they all store it. Forever.

Cryptocurrency breaks that chain. Not perfectly—blockchain analysis is a thing—but enough to decouple payment from persistent identity. Especially when combined with no-email registration.

And for those who need traditional payments? We support Stripe. Because pragmatism matters. But we don't pretend that credit card payments are anonymous. We're honest about the trade-offs.

What Anonymity Isn't

Let's be crystal clear about what we're NOT claiming:

Anonymity ≠ Impunity
If you use our servers for illegal activity, law enforcement can still investigate. They just can't start with "who owns this account" because we can't answer that question.

Anonymity ≠ Security
Your credential is just a random string. If you save it in plaintext on your desktop, that's on you. Anonymity from us doesn't mean anonymity from your own bad opsec.

Anonymity ≠ Invisibility
Your server has an IP address. Your proxy connections are visible. We're not

magic. We just don't tie those technical identifiers back to your personal identity.

Anonymity ≠ Zero Trust Required
You still have to trust that we're actually doing what we say. Open source code, transparency reports, and independent audits help, but perfect trustlessness is impossible in hosted infrastructure.

Anonymity is about limiting the damage when trust fails. It's about architecture that can't betray you even if the humans running it wanted to.

Why This Matters

The internet is splitting into two worlds: the authenticated web and the anonymous web.

The authenticated web is where governments and corporations want you. Real names. Verified identities. Traceable payments. Every action logged and analyzed. It's convenient. It's personalized. It's surveilled.

The anonymous web is where privacy still exists. Where you can explore, experiment, and communicate without building a permanent record. Where your data can't be weaponized against you because it was never collected.

Every service that requires real identity for no technical reason is pushing you toward the authenticated web. Every credential-based, no-email, crypto-accepting service is keeping the anonymous web alive.

This isn't about having something to hide. It's about refusing to live under constant surveillance as the default.

The Bottom Line

> *Privacy is when they promise to protect your data.*
>
> *Anonymity is when they never had your data to begin with.*

That's the difference, that's what we built, that's real anonymity.

A 32-character string. No email. No identity. No bullshit.

Everything else is just marketing.

Share this article

Twitter Facebook LinkedIn

More Articles

Behind the Firewall: Our Journey to a No-Logs, No-Compromise Platform

Nov 14, 2025

Quick Links

- Home
- Datacenters
- Servers
- Proxies
- Blog
- Partner Program
- Tor Mirror

User Panel

- Dashboard
- Deploy
- Billing
- Support
- Settings

YBC Holdings Inc.

8 The Green #21259
Dover, DE, 19901
United States

- Privacy Policy
- Terms of Service