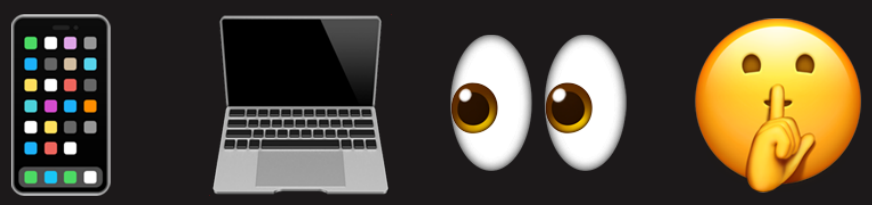
HLOCKWOO.COM

ARE YOU PROTECTED FROM DIGITAL SURVEILLANCE?



I spent yesterday afternoon setting up a more private digital life.

Given what's happening here in MN right now, I’m sharing the how and why of it all because our digital security matters more than ever.

(Scroll & save this post for receipts and actions you can take.)

WE ARE BEING TRACKED.

This is real, here's why:

- **ICE is using facial recognition** 🤳, stingrays that impersonate cell towers, and neighborhood-wide surveillance tools across Minnesota
- **ICE bought access to a phone surveillance** system that tracks movements of our smartphones, watches and other devices by using commercially purchased location data
- Minnesota AG **Keith Ellison issued a formal consumer alert** 🚨 urging Minnesotans to protect their digital privacy from DHS overreach
- **These tools don't just target immigrants.** They sweep citizens, protesters, and observers into the same surveillance dragnet

Sources: Sahan Journal, Minnesota Reformer, MN Attorney General's Office. Links to sources in caption.

HLOCKWOO.COM

THIS IS AN ISSUE FOR ALL US CITIZENS

THE DATA BROKER PROBLEM IS BIGGER THAN ICE

- Data brokers 👨‍💻 are a $250B industry built entirely on your information*
- Government agencies now buy your location 📍data instead of getting a court order, bypassing the Fourth Amendment**
- Dozens of data brokers collect the precise movements 🚶‍♂️ of hundreds of millions of people without their knowledge or consent***
- Foreign entities can purchase detailed personal profiles 👤 on US citizens for pennies****

This isn't paranoia. This is the business model.

*Sources: *Brennan Center **The Intercept, May 2025 ***EFF ****CFPB*

1: FIX YOUR EMAIL

Gmail is free because you are the product. Google's business model is knowing everything about you.

Solution: switch to Proton Mail.

- End-to-end encrypted, even Proton can't read it
- Based in Switzerland 🇨🇭 where they have the strongest privacy laws in the world
- Makes it easy to set up and use your custom domain for an email address that is your own

Full disclosure: I set this up yesterday afternoon. It’s going to take time to get completely off Gmail since it’s embedded in my accounts. But I've started the process of migrating. Starting somewhere is the point.

WHY PROTON

There are a lot email options so I did my research.
Proton stood out as the most secure option because:

✅ Open source, the code is publicly auditable
✅ Switzerland-based, outside US jurisdiction
✅ No ads. No data mining.
✅ VPN + password manager included in one plan
✅ Non-profit origin, mission-driven, not ad-driven

❌ Gmail = Google's ad machine
❌ Outlook = US jurisdiction, Microsoft ecosystem
❌ "Free" encrypted options are often unproven

When a company's revenue doesn't depend on your data, you're not the product.

2: CHOOSE A VPN WISELY

Many VPNs don't actually protect you.

Avoid:

❌ Free VPNs because they can sell your data
❌ US-based VPNs, they are subject to governmental data requests
❌ Un-audited VPNs, you're trusting their word
❌ VPNs owned by ad companies **(this is real and common so beware!**)

Use a VPN that is:

🇨🇭 Swiss or 🇮🇸 Icelandic-based
🔎 Independently audited and open source
📪 Funded by subscriptions, not advertising

I use Proton VPN. It's included with my email plan and qualifies by the above.

#3: CONSIDER VIDEO CONFERENCE OPTIONS

IT MIGHT BE TIME TO 🗑️ DITCH ZOOM 🗑️

Why? Zoom routed calls through Chinese servers and lied about end-to-end encryption. Now they want to use your meetings to train AI.

My advice?

- Switch to **Jitsi Meet**, it's free and open source
- No account is required to join
- It works in your preferred browser
- There is no corporate surveillance baked into the model
- When hosting a Jitsi meeting, remember to set a password & enable a waiting room.

#4: DON’T FORGET YOUR WEB BROWSER AND PHONE

CHROME = GOOGLE
GOOGLE = ADVERTISING SURVEILLANCE
YOU DO THE MATH

💻 **For your desktop browser:**

- Switch to Firefox & add uBlock Origin 🛡️
- Search with DuckDuckGo 🦆

📱 **On your mobile phone:**

- Settings → Privacy → Tracking → OFF
- Audit app permissions, revoke when unnecessary
- Most likely, your weather, navigation, store and coupon apps are harvesting your location and selling to brokers
- Use a password manager and stop reusing passwords.

FINAL THOUGHTS

I still have a public blog as well as Instagram and Threads accounts. I know the risks. I understand the trade-offs. Social media and community is important to me so I'm staying and publishing.

That said, there's a difference between what I put into the world intentionally through public posting and what's being quietly harvested from my behavior, location, and inbox **without my consent.**

"Data is being weaponized by a hostile federal government — and that was always the intended use for all that data collection."
— ACLU Minnesota

In summary, it’s in our best interest to lock down what we can. Start the process. Stay vigilent. ✌️