HEADLINES

How to “Opt-Out” from the Big Tech Social Credit System

12 crucial steps you should take now to protect your identity, assets, and sovereignty from Big Tech elites.

MAR 15, 2025

This article originally appeared on Door to Freedom and was republished with permission.

Guest post by Ryan Rivera

For those who aren’t familiar with the topic, the Communist government of China has implemented a “scoring system” to gauge the “trustworthiness” of individuals and business entities in China.

Chinese citizens are monitored and surveilled in real-time, with consequences being potentially dire. This score is tied to what services you can access in society, including employment opportunities, the ability to use transportation systems, and access to government services.

While we may think that something so Orwellian cannot occur in the United States with its vibrant history of democracy and open freedoms, as talked about in this

article, this system is already here. It has been quietly implemented through the corporate business community. Big Tech companies have long been willing to abuse terms of service agreements for their own benefit. Tl
new high after the COVID-19 pandemic.

The business community has embraced a culture of '
willing to utilize forceful practices like censorship, b
accounts to “dissuade” its customers from misbehavi

But, even more disturbing, secret government coerci
(such as the Biden administration’s collusion with Fa
pandemic criticism) raises a specter that threatens ou

We need to reduce our reliance on Big Tech and othe
Remember, *you can only be controlled only to the extent
services.*

12 Crucial Steps to Protect Your Identity, Assets & Sovereignty

Here’s what you need to do now to protect yourself:

1. ***Start using email services that protect your privacy*** – Use email services like Protonmail or Vivaldi that emphasize privacy. Google’s Gmail service is not “free.” In return, you provide them data that will be used to build a marketing profile of you and will be fed into their AI systems. I had previously recommended Tutanota but there are circulating rumors that its employees read user emails so I’d wait and see before endorsing it.
2. ***Stop using Google or Bing to do web searches and use one of the following alternatives:*** Brave Search, Metager, Ghostery, Qwant, Mojeek, DuckDuckGo, or StartPage. Comparing and contrasting these would take an article in and of itself and you should take the time to research the differences. DuckDuckGo is probably the most mainstream out of the above list, but lately, they have developed closer ties to Microsoft and are using more search results from Bing which has greater amounts of censorship. I’m not saying to stop using it but just to be aware and maintain caution.

3. *Stop browsing the web using Google Chrome or Microsoft Edge* – Neither Google nor Microsoft cares about your privacy. Instead, take the time to install and use a more secure alternative like Opera, Waterfox, Brave, Epic, or the grand-daddy of browser privacy, Tor Browser. Note Brave is built upon the open-source version of the Chrome browser called Chromium. Some caution is warranted as it is still possible for Google to place “backdoors” that may inadvertently be incorporated into Brave.
4. *Prefer Rumble, Odysee, or Bitchute for watching videos, and install Adblocker when watching on YouTube.* They are alternative video-sharing sites to Youtube. However, they have yet to match Youtube’s breadth and quality of content. At the least, you should use Brave browser plus install the Adblocker extension to block those annoying ads. Note Google is taking steps to crack down on Adblocker so this may or may not work in the future.
5. *Ditch any cloud storage solution without zero-knowledge encryption* – Sorry Google Drive, Microsoft cloud storage, Amazon Drive, and Apple iCloud, but you don’t make the privacy cut. These services still allow Big Tech to look at and audit your content. Instead, opt for a service that has zero-knowledge encryption in which the company cannot look at your content. There are numerous providers listed in this article, but some examples are Sync, Icedrive, and Tresorit.
6. *Ditch non-secure photo-sharing services and opt for one with privacy built-in* – Using Google Photos, Instagram, Facebook, Flickr, and the cadre of mainstream photo-sharing services exposes you to Big Tech holding your photos hostage. Instead, use a photo-sharing service that emphasizes privacy, like Smugmug or Cryptee.
7. *Opt to use secure video-conferencing that safeguards privacy* – Many of us who have gotten used to using Zoom for video-conferencing were disappointed by the recent announcement that Zoom will now start feeding your data to AI. Instead, use privacy-oriented videoconferencing like Jitsi and Whereby.
8. *Stop using your Google and Facebook IDs for signing into other websites* – The more we rely upon centralized web identification for signing onto websites, the more dependent we become. You do not want to get locked out of essential websites if Google decides to cancel your account. Instead, create individual accounts for all websites.
9. *Stop using Amazon and order directly from providers or buy locally* – Many of us have become reliant upon shopping on Amazon for our goods, and this makes us dependent on a central provider. Instead, order directly from the websites of providers, say Walmart.com, Target.com, or BarnesandNoble.com, or better yet, aim to support brick-and-mortar businesses.
10. *Aim to use cash whenever you can* – Credit card companies track our spending usage and use that data to feed into their AI systems or sell your info to third-party

marketing companies. Cash is king in that it cannot be tracked. Aim to use it whenever you can to support brick-and-mortar businesses.

11. ***Store local copies of all your data on multiple external hard drives*** – You should keep all copies of your data and photos on local external hard drives. It’s easy to purchase terabyte-sized storage from Seagate and back up all your data. It is essential you keep multiple copies for redundancy.
12. ***Think decentralization and redundancy for all your usages*** – The Navy Seal dictum *“One is none, two is one”* applies here. If you only have one of something (say email, photo storage, video-conferencing solution, local external storage, etc.), then you are unprotected in terms of failure. You need multiple copies of everything. I like to have at least three copies of any important data.

You may find the above daunting. You might be thinking, “Where do I start?” I’d advise to start small. Just pick something on the list above and just *look into it.* You can install the tool or read about how the tool helps protect your privacy better than the “mainstream” equivalent. Then, slowly switch your usage over to the new tool.

By implementing the above solutions, you can drastically reduce your reliance upon Big Tech and protect yourself from their efforts at coercion as they roll out their social credit system. By taking this time now and learning how these systems work, you can increase your level of freedom and protect your identity, assets, and security.

Remember the modus operandi of the Big Tech companies. Their aim is to *create dependence* so that whatever tool they offer becomes such an ingrained part of your life that you are willing to trade your privacy and ultimately your freedom for it. They directly make revenue from your usage.

Because we cannot trust Big Tech companies, it is up to us to educate ourselves on technology and how to use these tools. It’s not hard! It just takes a little time and effort, but then you will be protected. Decentralization and redundancy are the key considerations.

The power has always been ours to *disconnect* and thereby deny these Big Tech firms the attention and revenue that is their lifeblood. By collectively taking action, we send a powerful message to Big Tech that their machinations in our lives will no longer be tolerated.

Power and freedom then return back to the individual, arguably where it should remain.

The Vigilant Fox

Writer, video clipper, and pro-freedom citizen journalist with 12 years of healthcare experience. Tyranny is not possible without compliance.

Type your email... Subscribe

11 Likes · 4 Restacks

← Previous Next →

Discussion about this post

Comments Restacks

Write a comment...

Whocanibenow 3d

This is an ok post. I have a couple of points to add, based on my 15 years experience in IT Security. This comes from an auditor's perspective.

The first point is about Seagate. There are grounds for concerns about Seagate's neutrality in the hardware provider space. If you choose to use them, be sure to reformat and partition the disk before using. Do not use any software they provide for backups or anything. This is pretty much true for anyone. Recommended storage providers include Sandisk and Kingston.

A broader point surrounds this advice in general, which I contextualize as "Convenience versus Security." I have had untold numbers of conversations with end users, sys admins, dba's, IT Director's CTO's, CEO's and regular old people.

Almost universally they all want the easiest, cheapest solution. Like Vaccines, they just want someone to tell them it's safe, keep on following the path of least resistance.

I found it to be a losing battle. Those who know, know, and those who don't, don't really care.

Pretty good advice overall, but there is a hidden danger. There is also mapping and monitoring "out of band" behaviors, so people who slightly participate, inconsistently dis participate, and those who drop offline entirely are easily traceable as outliers. Damned if you do, damned if you don't.

♡ LIKE (2) REPLY SHARE

Mckeekitty 3d

All fine and good until reality sets in...

We're screwed!

LIKE REPLY SHARE