

Digital Privacy 101: No More Excuses

Transcript from a live webinar given by Sean Patrick Tario in May 2026



Thank you for joining. I'm going to be going through a lot of content tonight to get you a little educated and a little motivated to take action on something that is absolutely critical right now.

Before I start, I want you to know that we do free privacy consultations. So if you're going through all of this and you're thinking, "Man, I have so many questions, I just need to talk to somebody live, one on one," you can go to our website and book a free consultation. We spend most of our time on the phone, talking one on one with customers about digital privacy.

Because, as I'll dig into in the content, our digital privacy is very much the same as our physical privacy and security. What's the perfect fit for somebody is not the perfect fit for everybody. But I'll talk about that later.

Who Am I?

A graphic with a dark blue background featuring a grid of small dots and several large, overlapping blue circles. In the center-right, there is a circular portrait of Sean Patrick Tario, a man with a beard and short hair, wearing a dark suit jacket over a white shirt. Below the portrait, the text "Sean Patrick Tario" is written in a large, white, bold font. Underneath his name, several lines of text describe his roles: "Entrepreneur. Author. Investor. Technology Trainer. Husband. Father. Warrior for Truth in Love." followed by the URL "https://truthinlove.substack.com/". Below that, it lists "Data Center & Cloud Infrastructure Specialist. Chief Privacy Advocate & CEO, MARK37.COM" and "CEO, Open Spectrum Inc." In the bottom right corner of the graphic, there is a small version of the MARK37.COM logo.

My name is Sean Patrick Tario, and my background is as an entrepreneur in high tech. I come out of Chicago, born and raised. I went to Silicon Valley for university in 1998 and was there for the tail end of the tech boom, and I definitely witnessed the bust. I was a junior and senior in college when everything went to crap.

I was actually an assistant to a paralegal at a law firm off Sand Hill Road in Palo Alto when all of that happened. I literally watched the Lamborghinis and the Porsches that used to travel down that street every day turn into old, beat-down cars almost overnight. It was fascinating to watch.

I started a company when I was a sophomore in college and got the bug for it. I had a long career as an entrepreneur while also working for high-tech companies. I started working for data center companies, the things that are big news these days, and I eventually wrote a book about the data center industry because I was so fascinated with it and wanted to make it accessible to everyday people.

The book is called the Data Center Colocation Industry Playbook. It's basically data centers for dummies. If you're hearing all this news about data centers, what they are, how they operate, and how they work, and you want to learn a little more, I wrote this book years ago and it's still relevant today. You can go to any search engine and type in "Data Center Colocation Industry Playbook," or just look up my name, Sean Patrick Tario, and you'll find it online.

A little more about me personally. I've been married almost 21 years and I have three kids. My oldest is 19, my youngest just turned 13, both boys, and I have a daughter who just turned 17, which is mind-boggling to me. Father, husband, entrepreneur, author, investor. I've been investing in seed-stage startups for the last 20-odd years, always putting my money back to work, either in my own businesses or other people's ventures. So I put my money where my mouth is. I spent a little time working for large corporate companies, made a lot of money in a very short period, and realized that was not the home for me. I got out as quickly as I could to go back to working for myself.

What got me interested in digital privacy is simple. For a very long time, since I was probably 14 years old, I had a father who was very much awake, very much red-pilled. He forced me to watch documentaries. The one I'll always remember is called The Money Masters. If you haven't seen it, you can look it up; it was produced a long time ago. It's basically the video version of G. Edward Griffin's book, The Creature From Jekyll Island, which I read shortly after watching the series.

It teaches you about the history of money and banking, and that you have to follow the money. What my dad taught me is that you don't just follow the money to see who owns and operates a company and who holds the equity. You also have to figure out the ethos of those people. If you

understand the core values of the people owning and running a company, you'll learn how they're going to run that business.

If they're only about money, and they think they're gods on earth, they're going to treat that business, and treat you as a customer, the same way a psychopath would. Because many of these people are psychopaths, especially those at the IMF, the World Bank, and the Federal Reserve, which is neither federal nor a reserve. Same with big pharma, big tech, big banking, big anything. At that scale, the vast majority of the people believe they're gods on earth. They're in it for power, influence, and money. They're not in it to serve Christ. They're not in it to be servant leaders or stewards of the blessings bestowed on us by our Creator. They're in it for far different reasons, and they act accordingly.

As I started doing that in the data center industry, I noticed all these private equity firms gobbling up and controlling these companies, and it became obvious they were going to push hard to deplatform and demonetize anyone with ideas, thoughts, or opinions that ran counter to their narrative. I started warning people about this around 2014, 2015. Everyone thought I was crazy, especially in Silicon Valley. They called me a conspiracy theorist. I'm a conspiracy realist.

I was the one back when 9/11 happened, pointing at the screen saying this was a massive psyop, that these were clearly controlled demolitions. When they held up the passport they said the FBI found on the streets of New York from one of the hijackers, people believed it. I'd say, how do you believe a passport ends up intact on the ground after those massive fireballs? People were like, "Oh, that makes sense." I've been called a conspiracy theorist my whole life.

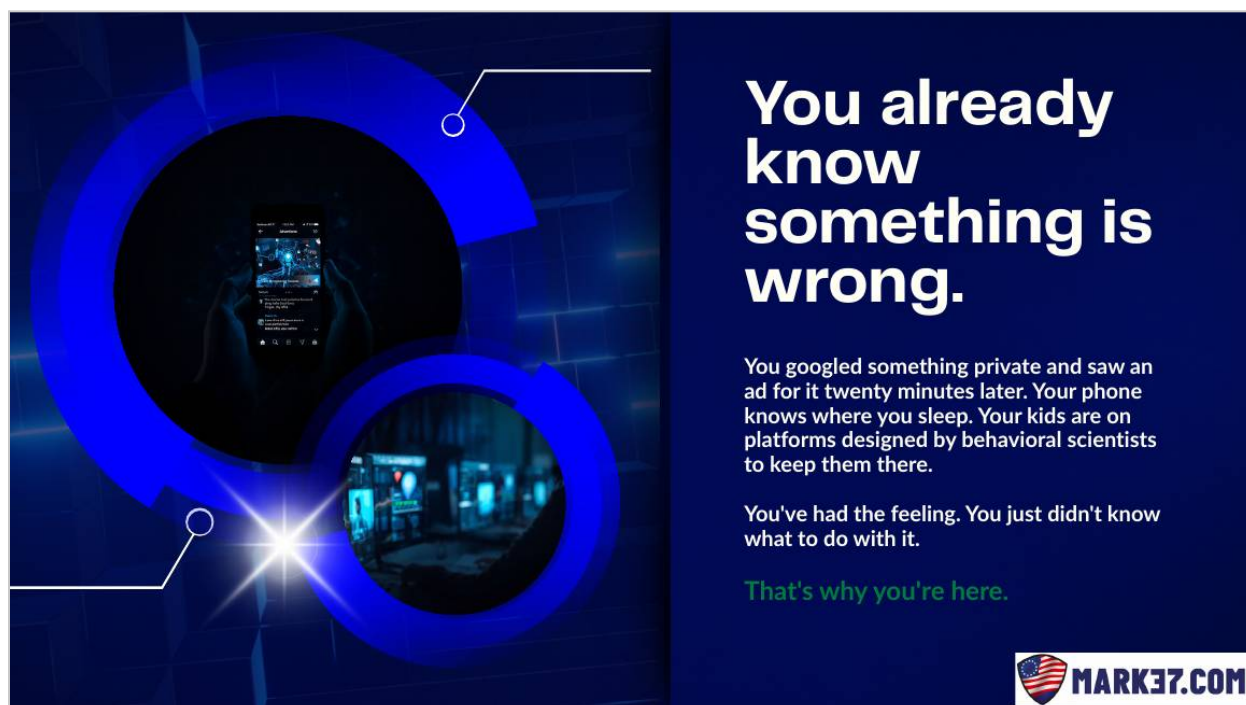
So I dug into the data center industry. I had a podcast called I Love Data Centers, where I interviewed the people who started the industry and built the internet. I had a lot of close friends in that space, and I started sorting out who were the psychopaths and who were the normal people. When Parler got deplatformed around January 6th, that's when the light bulbs really went off. When Trump got pulled off Twitter, and huge numbers of people got pulled off Twitter and Facebook, that's when people said, "Holy crap, you were right, Sean. This is happening. What do we do about it?"

I helped start a company called RightForge, which hosted Project Veritas. We were the original hosting provider for Truth Social. We had pro-life websites that got kicked off GoDaddy and other platforms come over to us. That company is now called American Cloud. You can go to americancloud.com. They're an Amazon Web Services alternative for companies building infrastructure online who want to work with God-fearing patriots who will defend your First Amendment rights to the death.

So as an entrepreneur I asked, now that we have facilities we control and own, ones they can't just flip a switch to turn off, what's the next major problem to solve? And it's the fact that everybody is carrying around devices running operating systems and software owned and controlled by the same psychopaths we claim we're trying to fight. That makes no sense.

So I started asking simple questions. If we don't want to use Windows, iOS, macOS, or Google Android, what can we use? I did the research and found Linux, which has been around for 30-some-odd years. I found GrapheneOS, which has proven to be the most hardened, private, and secure mobile operating system available. At that time, you kind of had to be a geek to use those tools. So I asked, what do we need to do to make these tools accessible to everyday people, so that my dad, one of the least tech-savvy people on the planet, can pick them up and use them without calling me for tech support every day? That's the impetus behind MARK37.

You can go to the About Us page at mark37.com/about to learn where the brand name came from. It comes from scripture. It's Mark 3:7, chapter three, verse seven, not "Mark thirty-seven." Go read about why we named the business what we did.




You already know something is wrong.

You googled something private and saw an ad for it twenty minutes later. Your phone knows where you sleep. Your kids are on platforms designed by behavioral scientists to keep them there.

You've had the feeling. You just didn't know what to do with it.

That's why you're here.



You're here today because you know something is wrong. If you're part of the John Birch Society or you read *The New American*, you're very aware of what's going on. I've been a member of those organizations for a long time. We know something is wrong. We know that when we say or talk about something near our devices, we get ads for it. And what's crazy is you can turn your devices off completely, have a conversation, and still get ads for the things you were talking about. Even

with the device off, you're still being listened to, monitored, and tracked.

What We're Going to Cover

What We'll Accomplish Today

This is not a scare session.
We'll cover the problem fast
then spend most of our time on solutions.

- How the surveillance economy works (and why it's accelerating)
- The tools that exist right now to get you out
- How to actually do it step by step - starting today



Let me tell you what I'm going to tell you. We're going to walk through the surveillance economy, because to this day people don't get it. I've been on three podcasts earlier today talking about this, and two of the hosts said, "I know this is bad, but what do I have to hide? So what if Google and Apple and Microsoft share my information? I've got nothing to hide." We're going to talk about the "so what," and why it actually matters.

Then I'll talk about the tools that exist right now, and give you some simple things you can do today that take minutes and will make you a lot more secure and private than you are right now. After that, we'll dig into solutions. I'll show you a whole range of options out there to whet your palate and keep you diving down this rabbit hole.

These Devices Were Designed to Enslave Us



I'm a big fan of The Lord of the Rings, and I'm sure some of you are too. There's a character, Isildur, who was a king. He fought a great battle and had the chance to throw the ring into the pit of fire and destroy it, and he chose not to. There's a great flashback scene where the king of the elves is with him saying, "What are you doing? Throw it in. You know this thing is evil. Get rid of it, please." And he doesn't do it. He walks away with the ring, and that begins the whole trilogy.

We have to realize that the things in our pockets have been designed to enslave us. The smartest people in psychology, sociology, and engineering have worked night and day on them for decades. They've spent trillions of dollars, and they're not hiding it. You can watch documentary after documentary where these people tell you they designed these things to be the most addictive products ever made, because they want your attention. I still meet engineers who say, "Well, they didn't know when they were designing these that they'd be used this way." Humbly, I think that's a load of garbage.

I'm a big sci-fi buff. Beyond Lord of the Rings, I've read every book in the Dune series, all 25-some-odd of them. I've read the first book close to 30 times; I read it every year. I've read all of Isaac Asimov, Aldous Huxley, Philip K. Dick, all the Star Wars. They have known since the early 1900s how this technology would be built and what it would be used for. They were futurists. They used systems theory and saw how things were progressing, so they could predict how it would all evolve. I remember as a kid going to Epcot Center with my family, seeing all the future stuff,

30-some years ago. We can't claim they just discovered they could use these things to manipulate, control, and psychologically abuse us. They've known for a long time.

Don't be like Smeagol.

Smeagol wasn't evil, but the ring changed him.
He became enthralled and addicted to it.
The Ring gave him something he didn't want to let go of, even when it was killing him.
Social media. Gmail. Convenience apps. They give you something real.
That's what makes them hard to leave... and the most addictive.
By design.

MARK37.COM

Here's another Lord of the Rings image for you. We also can't be like Sméagol, who not only holds onto the ring and is willing to kill for it, but jumps into the pit of fire to save the very thing he knows is killing him. I talk to people like this every day. They get such anxiety and angst at even the thought of walking away from iOS, or their Apple phone, or Google Android, or Windows. They have a fear they can't even describe. I have a dent in the wall in front of my desk from banging my head against it over the last couple of years, talking to people who understand all of these issues, know they're addicts, know they're addicted to these tools, and yet keep using them.

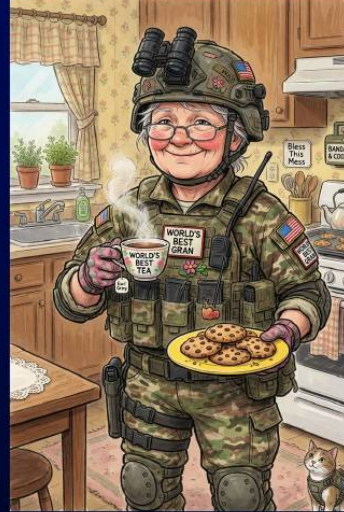
It's like being a doctor with a patient who's dying of obesity, telling him to please stop eating fast food three times a day, while he keeps going out and eating fast food three times a day. Or, I hate to say it, a lot of the talking heads and personalities in our industry are constantly out there telling you how bad big tech is, the surveillance state, the technocracy, and yet they keep using the very tools of the enemy they're harping on. That's like me telling you how evil Pfizer is, and then saying, "But hold on, I've got a booster appointment I need to get to." My credibility goes out the window. Everything I told you about Pfizer means nothing after that. It drives me insane. I feel like I'm taking crazy pills, living in clown world, when people say, "Yep, I see the problem clearly," and then go right back to doing what they were doing.

Grandma Doesn't Need a Grenade Launcher

Grandma doesn't need a grenade launcher.

She, and we, simply need better habits and tools not controlled by the very people we are trying to protect ourselves from.

Simpler is Smarter.



There are a lot of people out there pushing fear. “Buy this thing and you'll be safe. Use this VPN, this phone, this laptop, this security tool, and you'll be safe.” That's a lie, folks. It's like me telling Grandma that if she buys a shotgun and keeps it next to her bed, she'll be safe. If she doesn't know how to use it, when to use it, and she's not trained on it, she's more of a threat to herself and the people around her than any enemy who might come through the door.

Here's the point. These phones and laptops are psychological warfare weapons, and they have to be treated as such. A hammer can be a weapon or a tool that serves you. The difference is that you know how to use a hammer and when to use it. Same with a firearm. If I tell a firearms instructor, “I'm not gun savvy, I barely understand how it works, I get nervous around it, but I know if I pull the trigger it goes boom, so what should I carry on me all day?” any instructor worth a lick will tell you that you shouldn't carry, and you shouldn't even have a firearm on your person yet. You need to get trained, get familiar, and practice. Then we can talk about what's right for you.

The same concept applies to these devices. Big tech has sold and told us for decades that you don't need to know how it works. It's just so convenient, it just works, don't even think about it. They don't want you to know how it works, because the second you start learning, you start saying, “Wait, it's doing what? That's not okay. I don't want to use that.” It's no different than learning the ingredients in the food you eat. Once you learn that most of what you buy at fast food places or grocery stores is essentially poison, and you see how the big production houses process their

chicken, meat, and fish, you realize it's garbage food, fake food.

I've done an experiment with my kids where we ask, "Is this food?" and we leave it outside to see if the critters will eat it. We take two brands, one clearly processed and garbage, one organic, and leave them out. The processed stuff stays there. The organic stuff disappears. My point is, once you learn how this technology actually works, you have to make a decision, and you can't unlearn it. You also get smarter. It's the same operational awareness as picking your head up when you walk into a store or pull into a gas station and asking, "Is there a threat here I should be aware of, so I don't walk into a robbery in progress?" Because nobody has that digital situational awareness, and nobody's been trained on the basic 101, people are getting their digital heads blown off all day, every day, and they don't even know it.

The other key point with Grandma is that simpler is smarter. You don't need a million things to be safe. Sometimes a flip phone with basic functionality and a Garmin GPS for your car solves the whole problem. That thought alone blows our customers' minds. They say, "So I don't need the most technologically advanced psychological warfare weapon ever designed living in my pocket all day? I can get by with something simpler?" Yes, you totally can, and often you should. If you don't have the bandwidth, the time, or the desire to learn how these things work, then don't use them. That's totally fine.

People say, "But Sean, I still have to use my banking app." Great. Do it from the browser on a laptop you've secured in your home, and we'll coach you through how to secure that laptop. You don't need to be doing all of this from the phone you carry everywhere. My wife is a perfect example. God love her, I love this woman. She made a conscious decision to leave her phone on her desk. If she wants to see whether someone called or texted, she goes and checks it. She still operates like the phone is on the wall: if someone calls, she can go look. She's not getting triggered all day by every vibration, wondering who or what wants to reach her. And she's active all day, out in our garden, homeschooling our kids, keeping bees. For those who say, "Well, I need to have this," you don't. We got along just fine for a long time without all of it.

Stockholm Syndrome and Admitting the Addiction




Stockholm Syndrome

A psychological condition where captives develop a bond with their captors due to the power imbalance in the relationship. It is not weakness. It is survival instinct. Billions of people are not stupid for using Google, Apple and MSFT. They're rational. These platforms solved real problems.

The bond is genuine.

**Invisible chains are still chains.
A cage you choose is still a cage.**



You've probably heard of Stockholm syndrome, the psychological condition where you fall in love with your captors. That's where a lot of people are right now. They've fallen in love with the very companies trying to kill them, companies owned and run by psychopaths, some of them Luciferian psychopaths who want the destruction of you, your soul, and your family. We've fallen in love with these worldly things, and we have to acknowledge it. Raise your hand and say, "My name is so-and-so, and I'm an addict. They've successfully made me addicted to these things, to the point that I feel anxiety and angst and don't know how I'd live my life without them."

What blows my mind is that we just went through Lent. Almost everyone I know over the age of 55 said, "For Lent I'm giving up social media, giving up the news, giving up the constant feed. I'm going to spend more time in the Word and with my family." Every single one of them walked away from that experience saying they felt better, healthier, more connected to the people and things around them. And every single one of them went right back to the habits they'd felt free from. It does not compute for me.



The Joke... That's not a Joke

"My son asked me why I speak so softly in the house. I told him I was afraid the NSA was listening.

*My son laughed. I laughed...
Alexa laughed."*



Let me lighten it up with a joke that's really not a joke. My son asked me why I speak so softly in the house. I told him I was afraid the NSA was listening. My son laughed, I laughed, Alexa laughed. For those of you who have one of these things in your home, I hope you don't, but if you do, get rid of it. You've had the moment where you swear you turned it off and yet it's still on, still listening, still responding.

How Big Tech Makes Its Money

HOW BIGTECH MAKES MONEY

Every revenue stream is funded by you—either directly through purchases or indirectly through surveillance. You are not the customer. You are the product.

- YOUR DEVICE PURCHASE
- APP STORE & CLOUD CUTS
- TARGETED ADVERTISING
- GOVERNMENTS & THIRD PARTIES

MARK37.COM

Big tech makes money every which way, starting with the devices and hardware you buy. Let me drop a little tidbit. Every new phone is sold to you on a faster processor, a better camera, all these cool features. Most of those features are software features that can be pushed to your existing phone. You don't need a new phone for the vast majority of them. The real reason they want you to buy a new phone is that the new phones have more processing power, which lets them push the data collection and processing of everything they're aggregating onto your device, so they don't have to pay for it on their own servers. You're now paying more so that they pay less to make sense of all the data they collect from you all day. If that alone doesn't make you angry, I don't know what will.

Then there's the App Store. Every dollar you spend through Google's or Apple's app store, somewhere between 30 and 45 cents goes back to those companies, which is egregious. Then targeted advertising and the data brokers. You've probably heard of data brokers. The reason you might not even have the Facebook app on your phone, but you have a conversation near your phone and then see an ad for it on Facebook, is that they share all the data. They peer with each other and share it. And we clearly have governments and third parties buying that information too, not just companies that want to sell you things. Politicians buy this data. Our own government buys this data.

\$1 TRILLION A YEAR.

The combined annual revenue of Google, Apple, Meta, Amazon, and Microsoft:



Here's a massive point. Google, Apple, Meta, Amazon, and Microsoft, five companies, make over a trillion dollars a year combined. They spend billions annually on candidates, causes, NGOs, and organizations that are diametrically opposed to our values, that are trying to silence us and prevent us from existing online, lobbying Congress, state senators, and governors. On top of that, they employ millions of people, and the internal initiatives at those companies propagate that same agenda out to their employees, who then fund and support those causes too.

So when I hear, "Let's boycott Bud Light, boycott Target, boycott Liberty Safe," and everyone gets furious, nobody is talking about boycotting Google, Apple, Microsoft, and Amazon, the companies on the front lines controlling the media and the content you see. I had someone today say, "I make up my own mind. The device isn't controlling how I live." I asked if he'd ever been a politician. He said yes. I asked if he'd been censored. He said, "Yeah, I was deplatformed from YouTube and Google, hard." I said, so people couldn't find you, your campaign, or what you stood for, because the platforms prevented them from seeing it? He said yes. And I said, don't you see the connection? They absolutely influence what you see and what you don't.

This is one of the major reasons we live in a society where boys think they're girls who think they're boys who think they're cats, and we all play along. We have boys competing in women's sports with no major blowback. Why? Because a whole generation was raised in school systems and shaped by tools telling them this is normal and fine, and that if you don't think this way, you're a crackpot, a conspiracy theorist, a domestic terrorist.

There's a new list most of us are on now. It's called anti-technology terrorists. According to the FBI, we're anti-technology terrorists. This came out just two days ago. Every list you can think of, I'm on it, and almost everyone on my team is on it, and probably most of you too. So we can add that one. And I'm not even anti-tech. I'm anti-abusive-psychopath-tech. We're one of the few companies that will proactively tell you to stop using your devices, spend less time online, go live your life, get outside, do some grounding, grow something in your backyard. Anyway, I'll get off that rant.



Through the apps and platforms, your loyalty cards, your internet service providers, and public records, they have a complete profile. They have everything. I'm one of the few people who journals every day, and I've been doing it since I was 19. It's an awesome thing. I can go back and read my journal from when I was 19 and watch the evolution of my thinking. But even with all of that, if I were still plugged into the Matrix, and the Matrix still had every website I visited, every fraction of a second I paused on an ad, all my emails, all my texts, everything I've ever bought, it would know more about me than I likely know about myself.

How do you think they trained these AI models? By taking all the data, real-time video, and audio from the devices in your pockets right now, and feeding it into these systems. And you signed off on it when you accepted the terms of service from Google, Apple, and Microsoft. Nobody reads those terms, but that's exactly what you agreed to. You've been feeding the system. We have to stop feeding it. We have to opt out and walk away.

People tell me all the time, “But Apple says they're a privacy company.” Go read the white paper we have on Apple in the resources section at mark37.com. We tear Apple apart just by presenting the facts. They are lying through their teeth, and it's in the court cases and the documentation. They operate no differently than the financial firms that lie through their teeth, make billions, get fined fifteen million by the SEC, laugh all the way to the bank, and then go become chairman of the SEC. That revolving door is the same in big tech, with the FBI, the NSA, and the CIA moving back and forth between these companies. People ask how they get away with it. It's corruption, plain and simple. What's more insane is how people keep using these tools knowing all of this.

It's All About Owning Your Data

It's All About Owning Your Data.

Every item on this list is something these companies have confirmed they collect - through congressional testimony, privacy policy fine print, court cases or reverse-engineered apps.

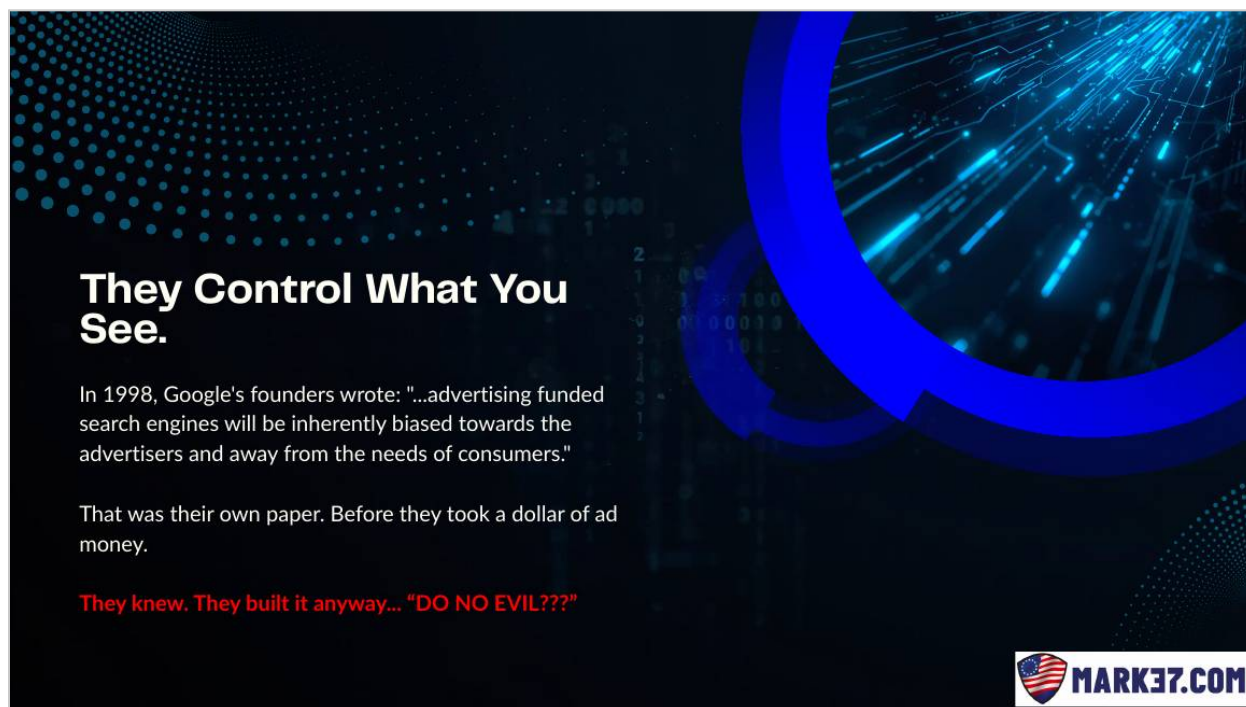
- WHAT YOU SEARCH FOR
- WHERE YOU GO & WHAT YOU BUY
- YOUR PREFERENCES AND OPINIONS
- WHO AND WHAT YOU INTERACT WITH AND WHEN

MARK37.COM

As a young entrepreneur going up and down Sand Hill Road, where I'd interned at a law firm before starting companies of my own, I had to go raise money. This was the early 2000s, and every single time we sat down with venture capital firms, they asked, “What's your data plan? What's your data strategy?” That was true through the late 1990s and even earlier. It has always been about data collection and harvesting.

The idea of building technology as a tool that serves only you, where you own and control your data, would not get funding. If you couldn't find a way to exploit, use, or sell that data, they didn't want to invest. You scratch your head and ask why. You follow the money and realize the same people hold controlling stakes in all the major venture capital firms and private equity firms. The

last edition of The New American broke this all down beautifully across about ten articles. This is not complicated, folks. It's been designed this way from the beginning. They control what you see, and they've known it from day one.




They Control What You See.

In 1998, Google's founders wrote: "...advertising funded search engines will be inherently biased towards the advertisers and away from the needs of consumers."

That was their own paper. Before they took a dollar of ad money.

They knew. They built it anyway... "DO NO EVIL???"



Google's own founders, Page and Brin, said it themselves early on: advertising-funded search engines will inherently be biased toward the advertisers and away from the needs of consumers. They knew it from day one, and then the big fat checks started coming in, and they put out "Don't be evil" as their slogan, which is a joke. One of my fraternity brothers from college went on to run advertising for the adult section at Google, which is how I learned that over 70 percent of Google's revenue, especially in the first couple of years, came from the adult entertainment industry.

It's also how I know, being in the data center industry, that the top systems engineers, network engineers, and programmers who knew how to build systems at scale, to grow infrastructure for tens and hundreds of millions and eventually billions of users, came out of the adult entertainment industry. There was no Amazon back then. Amazon didn't become the behemoth it is until 2004 or 2005. So the people who built the big adult entertainment companies got hired by Google, Apple, Microsoft, and Amazon to build and scale their infrastructure. Ethos matters. You can't tell me you're all about "don't be evil" when the vast majority of your money comes from porn. Those are facts. Go look it up.

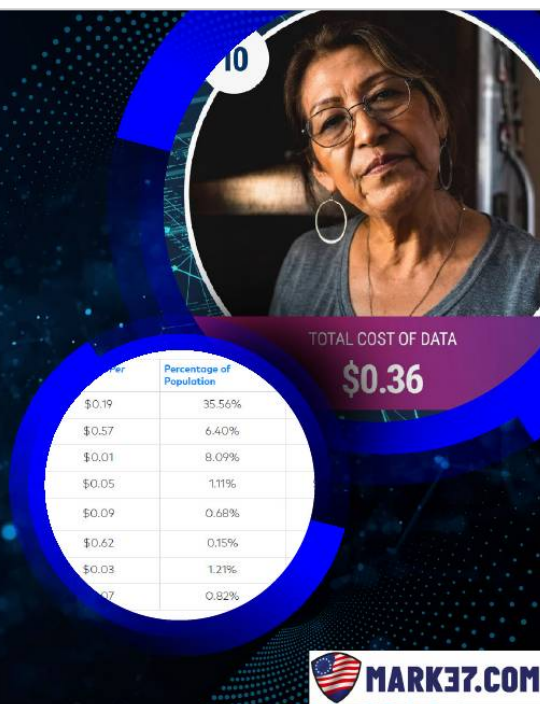
What Is Your Data Worth?

What Is Your Data Worth?

The average American's complete data profile sells for somewhere between \$150 and \$240 per year on the open data broker market. Google's revenue per user is north of \$300 annually.

You think you're getting free services. You're paying with something more valuable than money. You're paying with behavioral access - the ability to shape what you think, what you want, and what you do.

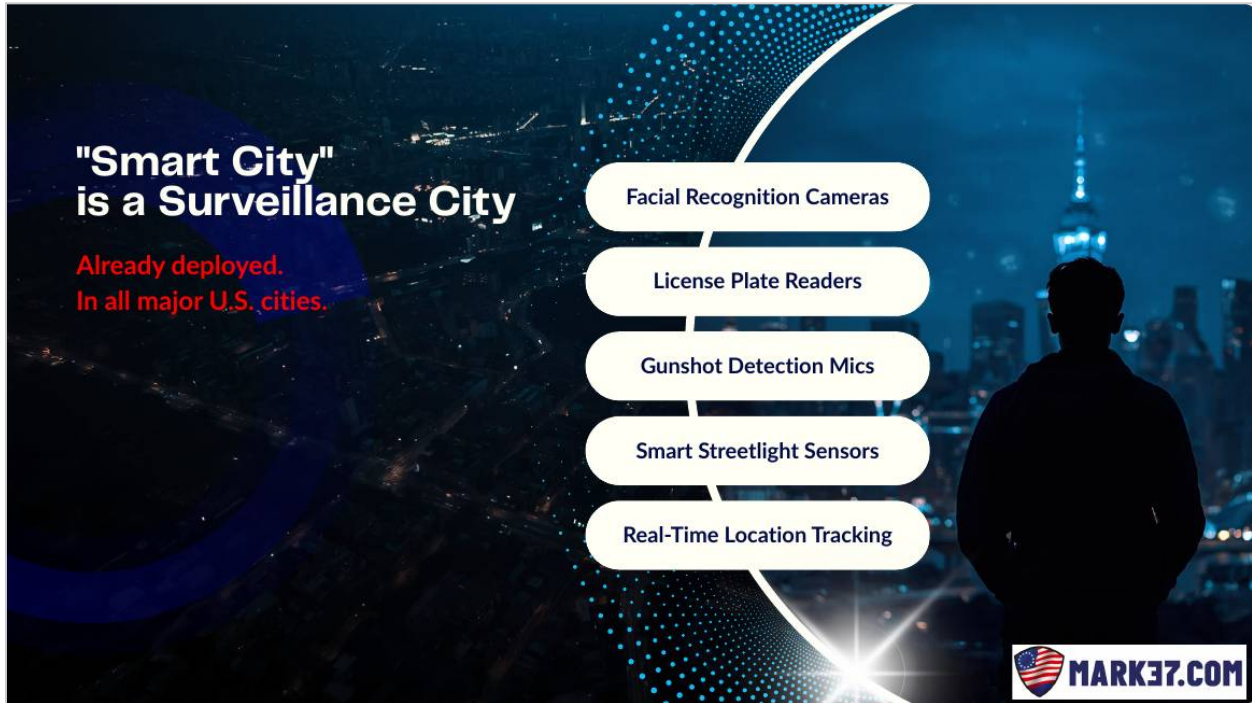
Your data is the product, and you are being sold.



People ask what their data is really worth. It's being sold all day, every day. Individuals and companies can work with third-party brokers to target specific demographics and push advertising or any messaging out to them, and then get information back. If you want usage metrics, if you want data on how a demographic is acting and reacting in the marketplace, you can buy all of it. Google's revenue per user is north of 300 dollars a year. They're making 300 dollars a year off you, and you don't even know it, all from the information you feed into their system.

You are the product. And understand this: privacy is not paranoia. The data brokers tout this stuff. Their entire sales pitch is how much information they have on the world and all the great things you can do with it. Your convenience is literally their control.

Smart Cities, Briefly



I won't go too deep here, but I give a whole presentation on smart cities. If you're worried about a smart city near you, reach out to me at sean@mark37.com. I've been traveling the country for the last four years giving these presentations. I did one in Myrtle Beach not long ago. I'll tell you, the player to worry about is not the government. The government is simply signing off on private companies coming in and putting up all the infrastructure. The county council members and mayors are clueless and not tech savvy. All they see is paychecks and dollars.

When you hear that Myrtle Beach, a designated smart city, has a big initiative to put sensors in garbage bins so the waste company knows which bins to pick up and save money, you realize they're not the player you need to worry about. It's the corporations. The city, the county, and increasingly the state are just signing off on all the surveillance. We need to educate them so they understand exactly what they're signing off on.

A Layer of Control

WARNING SIGNS OF ABUSIVE RELATIONSHIP

- ✓ Constant Surveillance
- ✓ Financial Control
- ✓ Gaslighting
- ✓ Forced Isolation
- ✓ Narrative Monopoly
- ✓ Blame Shifting
- ✓ Moving Goalposts
- ✓ Manufactured Dependence

Abusive Relationship

This is not a political statement but a pattern recognition exercise.

Ask yourself which ones describe your relationship with your government and the platforms it partners with.

15 Signs You May Be In An Abusive Relationship:
Isolation. Monitoring. Control. Gaslighting. Threats. Economic Abuse. Intimidation. Emotional Manipulation. Blame-shifting. Restricting Autonomy.

MARK37.COM

If you go through the warning signs of an abusive relationship, they mirror exactly what big tech is doing, and exactly what our government is doing to us, almost verbatim. It's not funny. It's sad.

It's Not Just About Advertising.

The infrastructure being built is not for convenience.

It is a control layer.

- CBDCs**

Programmable money that can be restricted by behavior or compliance status - live in 100+ countries
- Digital ID Systems**

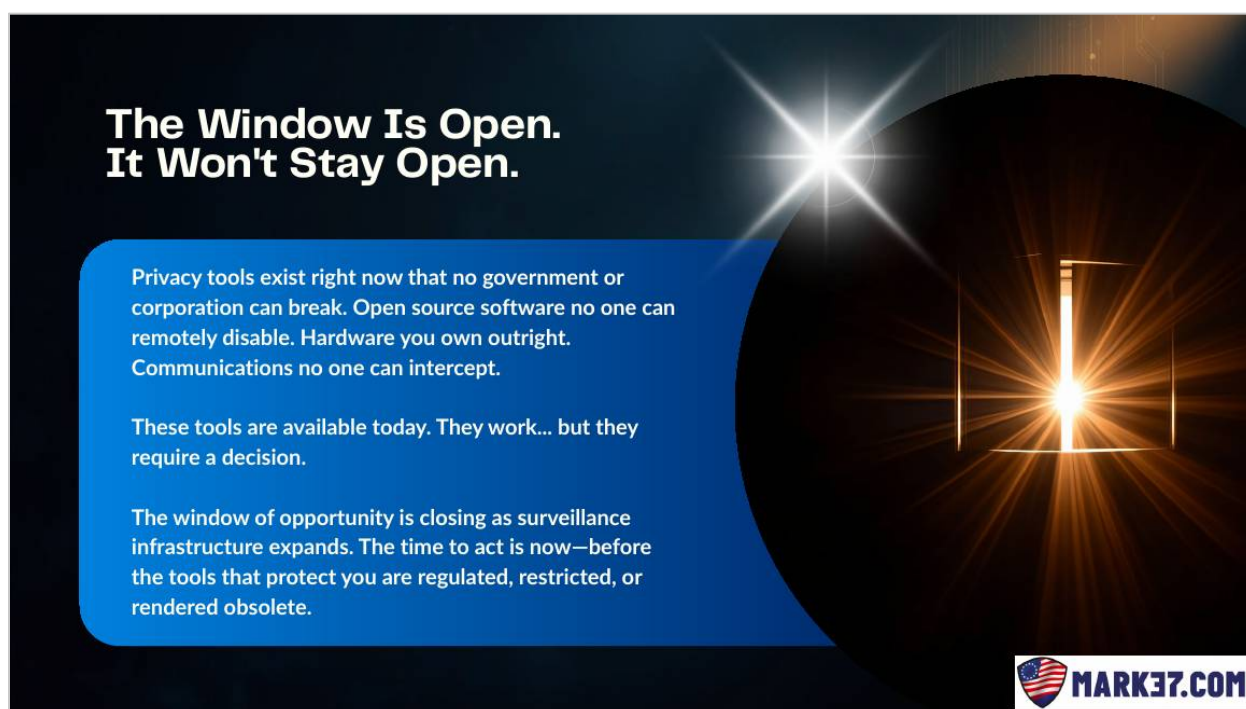
Systems tied to health, travel, and financial access being built across EU, UK, Australia, Canada
- Social Credit**

China's system is not a warning but a working model being studied globally

MARK37.COM

They've been building this layer of control piece by piece, and the current administration isn't stopping it. In fact, they're advancing it, which is mind-boggling. It's all about digital ID, and they're using China as the model for how they want to roll it out globally. Terrifying.

Every new car is a mobile tracking device. If you're considering buying a new car, please don't. You're literally signing terms of service that give the manufacturer access to your vehicle. That car you bought should be yours. It should serve you, not serve as a tracking device. And yes, you can go through and say you don't consent to them pulling your information. They don't care. They're going to do it anyway. That's exactly what Facebook, Apple, Google, Microsoft, and Amazon have done, and the courts have proven they've been lying about it. They make far more harvesting that data than they'll ever pay in fines, if it even gets discovered. And they want to tie it all to a social credit system.




**The Window Is Open.
It Won't Stay Open.**

Privacy tools exist right now that no government or corporation can break. Open source software no one can remotely disable. Hardware you own outright. Communications no one can intercept.

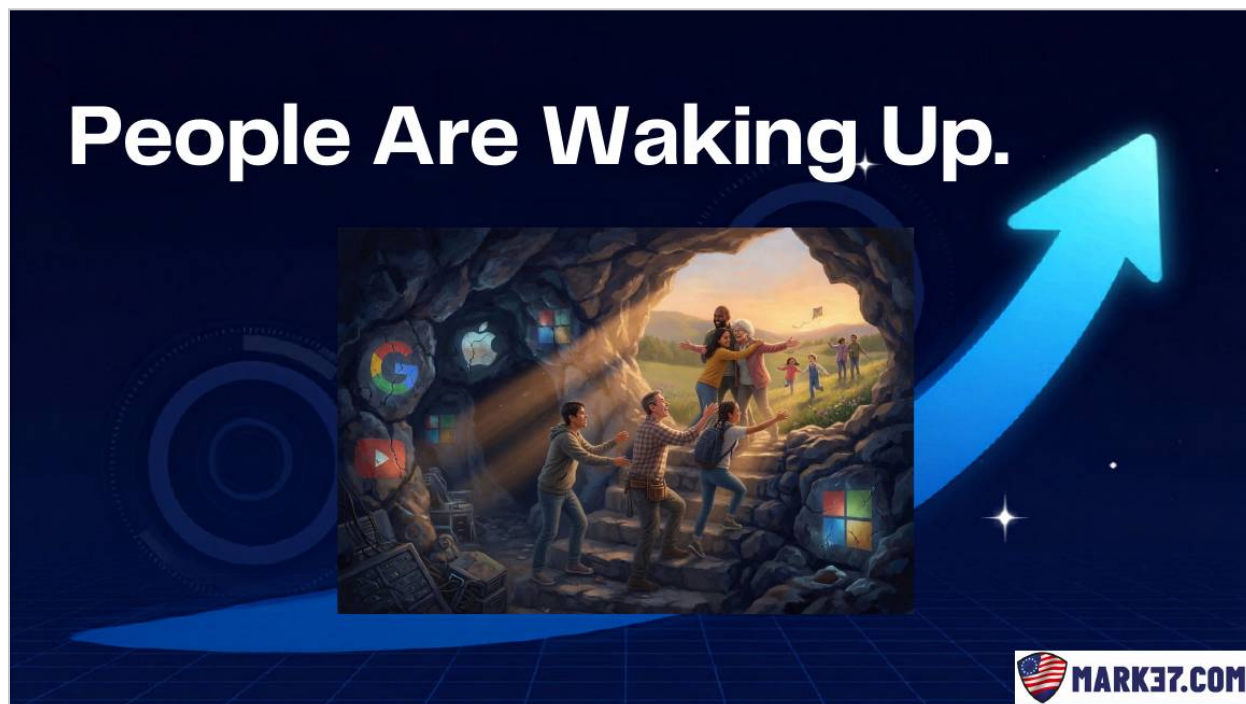
These tools are available today. They work... but they require a decision.

The window of opportunity is closing as surveillance infrastructure expands. The time to act is now—before the tools that protect you are regulated, restricted, or rendered obsolete.

 **MARK37.COM**

So we have to start opting out. The window is still open. I believe we've been blessed with a moment of reprieve before things get truly terrifying. We have a couple of years, at best, to start migrating and shifting our consciousness. Just as we have to start asking who can supply our local protein and produce that isn't poisoned, who can fix a small motor, who we can rely on in a crisis, we have to start doing the same with our technology. You have to start learning how to use tools that are designed to serve you, instead of being the product yourself.

The Good News: People Are Waking Up



The good news is that more people are using these tools every day. When I started this business in 2022, I was fighting an uphill battle. I'd walked away from a lucrative industry career because the Lord made it very obvious that wasn't where He wanted me. I've learned over my life that if I'm not obedient to God's will, He'll slap me upside the head and make it blatantly obvious what I need to be doing. So I used to pray, "Lord, make it so abundantly clear I can't ignore You." Now I pray, "Lord, if I'm not doing the right thing, gently make it clear what You want me to do."

Back then I was pleading with the Lord about why He had me doing this, because every conversation was an uphill battle. I could tell you story after story where my hope was waning. But things have really turned over the last year and a half. People are waking up in droves. We're starting to see the hockey stick. We're at that three to four percent mark of users actually adopting privacy- and security-focused products. If you know anything about marketing, you know that three to four percent is the sweet spot. When adoption hits that point, things take off, and that's exactly what we're seeing.

Privacy Is Winning.

- Signal: 100M+ users
- ProtonMail: 100M+ accounts
- Brave Browser: 100M+ monthly active users
- Brave Search: 20 billion annual queries and growing
- Linux Server: Powers 96% of the world's top 1M web servers
- Linux Desktop: Now 5%+ of U.S. computers - up 70% in 3 years. Over 780K Windows refugees switched to Linux.
- GrapheneOS: ~400K active users worldwide - zero marketing, zero telemetry.
- VPN Usage: 1.75 billion people globally now use a VPN. One in three internet users.



 **MARK37.COM**

Now, I'm not a huge fan of Proton Mail, and I'm not the biggest fan of Signal. But the fact that more people are using tools that put privacy and security first is a good thing. At least they're moving in the right direction. As we educate people about what's really happening, they can start using better and better tools.

Think of the prisoner in the cave watching shadows on the wall. That's where we live. We're living in the Matrix, folks, and our job as a business, and your job as someone listening, is to help people escape it. We're the Morpheuses and the Trinitities, reaching out to the Neos who have an inkling that something isn't right. Our job is to pull them out, show them the harsh reality, and then give them the tools to thrive and survive in the days to come.

You Can Opt Out. Completely. Right Now.

Not eventually.

Not after you become a tech expert.

Not after it gets bad enough to justify the effort.

People are using Ghost Phones and Ghost Laptops today who Google has zero data on.

Whose conversations are encrypted end-to-end.

Who run AI on their own hardware at home.

Whose carriers don't sell location data.

You don't need security clearance or a computer degree.

These are parents, farmers, business owners, retirees and pastors.

They just made a decision and took action.



I want to stress this: you can opt out completely right now. We have farmers, parents, and pastors who have done it. G. Edward Griffin is one of our customers, and we were with him this week helping him fully migrate off his Windows laptop. Most of you have probably heard of Mr. Griffin. He's the sharpest 90-year-old I've ever met, and his library is one of the most epic on the face of the planet. If he can do it, you can. We have people in their 90s who aren't as sharp as Mr. Griffin making this migration too. You can be a working professional; my entire business runs on open-source tools that respect our privacy. You have no excuse, and we cover all of it in our Q&A, our getting-started guides, and our documentation. The only real reason you can't do this is that you want to keep living in ignorance. After tonight, you either take the blue pill and keep eating the steak you know isn't real, or you say, all right, I have to do something.

Digital Privacy 101: Quick Wins

The graphic features a dark blue background with a network of glowing blue lines and dots, resembling a data visualization or a neural network. The text is white and light blue, with some words in red for emphasis. The layout is clean and modern, with a vertical line on the left side of each list item.

Digital Privacy 101

If your job, or life, requires you use technology, you should learn the basics!

- Don't install apps that harvest and sell your data.
Learn how to check for this.
- If it sounds like a scam... it likely is.
DO NOT CLICK. Always Verify.
- Do not log into random wifi networks.
Especially in hotels, airports, coffee shops, malls, and restaurants.
- Stop using tools owned by psychopaths.
Trying to control, enslave and kill you. This is not hyperbole.
- We don't need psychological warfare weapons in our pockets all the time.
Or in our cars and homes... all day every day.

Simpler is Smarter.

 MARK37.COM

If your job or your life requires technology, you need to learn the basics, for all the reasons I've already given. You have no excuse to keep using these tools, getting frustrated with them, and complaining about them without understanding how they actually work. That's why you're here. I appreciate you being here, and I'll try to stop yelling at you.

First, don't install apps that harvest and sell your data, and learn how to check for this. It's not hard. In the app store, before you download, it tells you exactly what the app wants access to on your device. You can also go into an app already on your phone or laptop and check its permissions. Does your flashlight app need access to your Wi-Fi or your contacts? No, it absolutely does not. But do you even know how to check whether it has that access? You should learn how.

Second, if it sounds like a scam, it probably is. It's election season, so like all of you, I get a dozen spam calls and texts a day from politicians, and even more from people who want me to take out loans. Don't click anything that comes through your device by text message. Verify. If anything comes in that's financial, verify by calling the number on your credit card or the number for your bank and talking to a live human you actually know there. AI has gotten so sophisticated that if you've already given an app access to your contacts, scammers know who your family members are, and they can even spoof a family member's phone number to plead for money. Your discernment has to go up if you're going to use these tools, or you're going to get scammed. Anyone who tells you to just buy this one thing and you'll be safe is lying. You have to get smarter.

We have a ton of articles on the website to help you build this discernment, including a whole article just on discernment.


Third, don't log into random Wi-Fi networks. This should be obvious, but stop logging into random coffee shop, mall, restaurant, airport, and hotel Wi-Fi. A hacker can easily set up a honeypot, a fake network with the same name as the legitimate one, and you'll connect because it's free. All you're doing is giving someone access to your devices. So what's the alternative? Use the data plan you already have. Set your phone up as a hotspot and route through it. I don't connect to random Wi-Fi unless I know the person and know they have their home or office locked down. I use my phone as a hotspot and route through it.

Fourth, and I've been yelling about this for the last hour, stop using tools owned by psychopaths. This is like handing a soldier a weapon in combat and saying, "By the way, all your communications, your GPS, and your position on the battlefield will be fed to the enemy you're about to fight." Would you use that weapon? No. You'd be a sitting duck. This is common sense, but we've been brainwashed into thinking it's normal. "So what if they have a little information about me? I'm not doing anything wrong." Does the Fourth Amendment matter? I'm not planning to shoot anyone, but my Second Amendment matters. I'm not planning to offend anyone, though I probably just did, but my First Amendment matters. I should still have privacy. If I said I was going to follow you everywhere you go and track everything you do, even inside your home, you'd get a restraining order. So why is it fine for Apple, Google, Microsoft, and Amazon to do exactly that? That's where I feel like I'm taking crazy pills.

Start Where You're Comfortable

Pick Your Level. All of Them Work.

- TIER 1**
DIGITAL HYGIENE
(Free. Today. Anyone.)
 - Replace your browser, email, and search engine.
 - Eliminates roughly 70% of passive surveillance.
 - Takes one Saturday afternoon.
- TIER 2**
HARDWARE SOVEREIGNTY
 - Microphone locks + Data Blockers + Faraday Bags
 - Ghost Phone + Ghost Laptop.
 - Eliminates Google and Microsoft from your daily life.
 - Your apps still work. Your number stays the same.
 - You disappear from their grid.
- TIER 3**
FULL OPERATIONAL SECURITY
 - Ghost Home + Sovereign MVNO + Encrypted Comms + Local AI.
 - You are running parallel infrastructure.
 - If the grid changes, you don't change with it.



You can start wherever you're comfortable. We've learned that people want checkboxes. They want to say, "Okay, I did this, what's next?" So we have guides and roadmaps on our website that coach you through the process at whatever level you're at.

You can start with the easy, cheap things. For about 20 bucks, you can get something called a mic lock that mutes your phone's microphone. You can get a Faraday bag, learn what it is, and use it appropriately. Or you can take the next step and change out the phone and operating system you're using, and swap the applications you depend on that are run by psychopaths for better alternatives. This is all about layers, and not everyone needs to be an expert.

These lunatics don't even let their own children use this technology. That's a fact, and they say so in their own documentaries. They don't let their kids use these tools because they know how addictive they are, and how much of a psychological warfare weapon they are.

The Future Is Local, Decentralized, and Open Source

Would You Buy a Car With a Welded Hood?

CLOSED SOURCE

The code is hidden. You cannot see what it does, who it reports to, or what it's designed to collect.


You are trusting the manufacturer completely - and the manufacturer has a financial incentive to surveil you.

OPEN SOURCE

Reviewed, tested, and verified by thousands of independent developers worldwide.

If there is a backdoor, someone finds it and lets you know, because they too depend on the code to be secure.

Transparency is the security model.

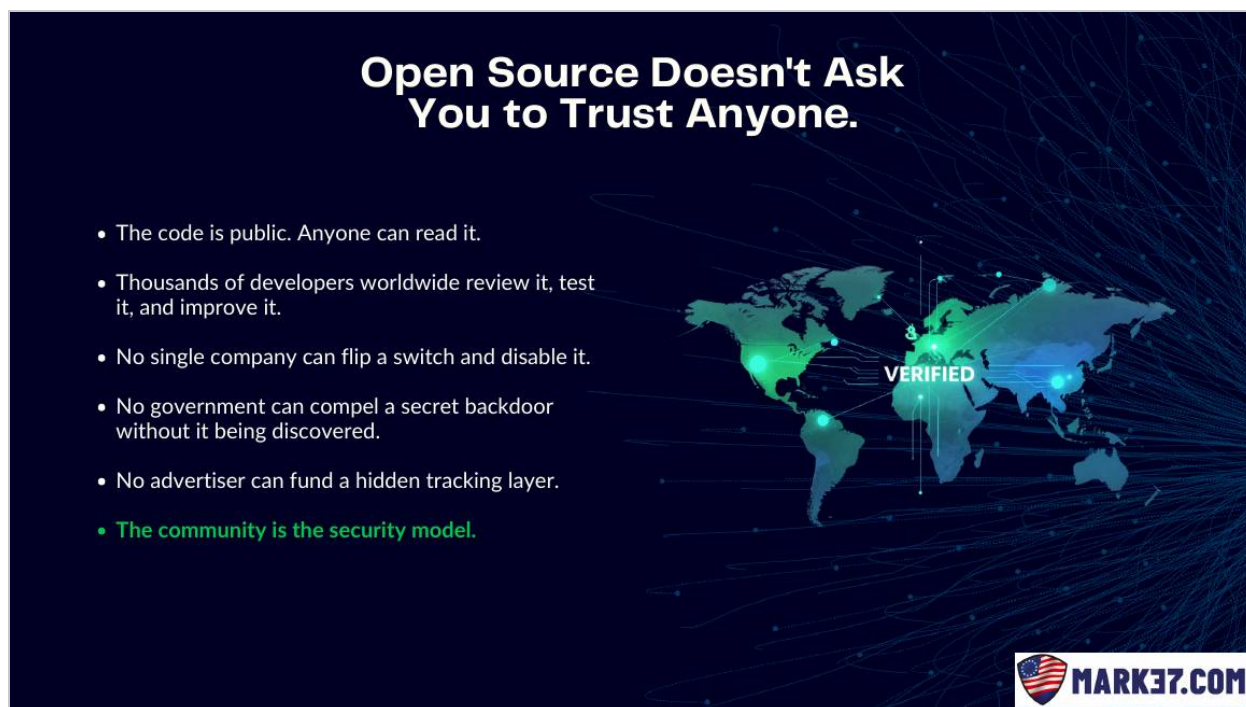


I'm a big proponent that the future is local, decentralized, and open source. Open source is key, and you have to understand what it means. Open-source operating systems like Linux have been around for 30 years. There's a reason more than 90 percent of enterprise servers run on Linux: it's open source. The development team, the systems engineers, and the network engineers can see, in real time, the code running their business. If something nefarious is happening, they want to pinpoint it immediately and say, "From one to two in the morning, our back door is opening up. That's a problem, let's fix it." That's very different from a company that says, "Just trust us, we've got it covered."

Open source doesn't mean thousands of people are managing it. There's still a core group responsible for the code. What it means is transparency. They show you exactly what's happening. In the analogy of your home, it's like having the full blueprints: you know where the electrical and plumbing run, and which door opened and closed and when. That transparency lets companies like mine verify that something marketed as private and secure actually is. A big reason companies keep things closed source is to protect intellectual property. I'd argue that all of our ideas come from our Creator, and the real value is in the execution. Ideas are a dime a dozen; I witnessed that in Silicon Valley. The execution is what matters.


So if I come up with a great idea about, say, zero-point energy, I'm not going to file a patent and wait for the government or some big company to show up, offer me a stupid amount of money I'll

refuse, and then wait for my convenient heart attack or car crash. I'm going to decentralize it as fast as possible and get it into as many hands as possible, so everyone can do something with it. I'll keep working to make it a real, living thing, and if people want to buy it from me, great, but I don't want to be the sole bottleneck for that information, because then I'm a sitting duck. Open source lets you do that.



Open Source Doesn't Ask You to Trust Anyone.

- The code is public. Anyone can read it.
- Thousands of developers worldwide review it, test it, and improve it.
- No single company can flip a switch and disable it.
- No government can compel a secret backdoor without it being discovered.
- No advertiser can fund a hidden tracking layer.
- **The community is the security model.**



Closed source, which is Google, Apple, Microsoft, and Amazon, is the opposite. Why are they closed source? A big reason is that if we could see their code, we could point and say, “Here's the back door that gives the NSA access. Here's the one that gives all these other people access. This is messed up, and you need to fix it before we'd even consider using your products.” So they keep it closed for a reason. The community is the security model: a community of developers, coders, systems engineers, and network engineers who care about these products, looking at the code, vetting it, testing it, and providing feedback.

Your Phone Is the Front Door to Your Life



Your Phone Is the Front Door to Your Life.

- Your location, 24/7.
- Your contacts and their locations.
- Your search history.
- Your camera and microphone – remotely accessible.
- Your banking apps.
- Your email.
- Your photos.
- Your voice recordings.
- It is the single most surveilled object in human history.

And you carry it everywhere you go.



Your phone is the front door to your life, and you carry it everywhere. Try this: next time you run a quick errand, get gas, or go to the grocery store, leave your phone at home. Get in the habit of not being tethered to it. That's basic and simple. And if you feel anxiety at even the thought of doing it, you have a problem, and that's okay. They've spent trillions of dollars making these things as addictive as they are. That doesn't mean you adopt a victim mentality and demand reparations. It means you make a change in your behavior. This is a lifestyle change, just like health and wellness or homesteading. What we're talking about tonight is a lifestyle change to defend and protect your digital privacy and security.



Little steps. Baby steps. This is a journey, not a sprint. Some people can sprint through it quickly and easily. For others it might take months.

A flip phone is a solid option, but I'd encourage you to sign up for a consultation and let us walk you through it. Really, you just have to do an audit. The first thing we ask people to do is audit their digital life. Document the apps you depend on. Then ask, do I need access to that from my phone? If you go down the list and realize you only really need the phone for calls and texts, then a flip phone does it. If you also want directions in the car, get a Garmin GPS. Problem solved.

What Is GrapheneOS, and What Is the Ghost Phone?

GrapheneOS: Android Without Google.

- Built on the Android Open Source Project (AOSP) - the same codebase that powers every Android phone.
- Google's tracking, telemetry, and data collection **removed**.
- Security: **hardened beyond stock Android or iOS**.
- App compatibility: full. Your banking app still works.
- Nuke your phone with a secret pin code
- Development: non-profit, open source, community verified.
- Used by security professionals, journalists, lawyers, and executives worldwide.



Years ago, when I started asking what would solve this problem, I found GrapheneOS. There were other options: LineageOS, /e/OS, Rob Braxman had his device. But none were as hardened, secure, and private as GrapheneOS. As more people, including security professionals, started using it, the consensus became clear. Do a search online: hands down, GrapheneOS is the most private, secure, open-source mobile operating system available.

Because it's based on Android, and most people don't know this, Android itself is open source. Google builds its version of Android on open-source Android, and there are now dozens of forks. GrapheneOS is one of them. The benefit is that any Android app will work on the phone. So the question is never, "Will this app work?" The question is, "Should I even be using this app in the first place?" That's the key. When you go through your list, you'll realize the answer is no for about 80 percent of those apps.

Same Number. Same Apps. Zero Google.

WHAT'S GONE

- Google access to your location
- Remote camera/mic access
- Unencrypted calls & texts
- Closed source firmware
- Contact & search history tracking
- Unsandboxed app data sharing

WHAT STAYS

- Your phone number
- Your contacts
- Your apps (maps, weather, etc.)
- Your user experience
- Your daily workflow
- Your peace of mind

The surveillance layer is gone. **The phone still works.**



You can keep your same phone number. Every carrier you use now is compatible. You can take the SIM card out of your current phone and swap it into the new one. If you have an eSIM, you call your carrier and say, “I have a new device, I’m bringing my own device. I need to move my eSIM over.” They’ll help you. So again, the question isn’t whether your carrier is compatible. The question is who owns the carrier, and what data are they harvesting? You keep your contacts, your maps and weather, and a user experience you’ll probably find familiar if you’re coming from Android. It’s a little different coming from iOS, but I promise that after two weeks you won’t notice. You just have to learn where to go to do the thing. When cars moved from a key in the ignition to a push-button start, I was the guy asking, “Where do I push the button?” It took a couple of weeks to get used to it. You’ll get used to this too, and you’ll walk away with peace of mind that you’re no longer freely giving away all your information to companies trying to kill us.

The Ghost Phone

- GrapheneOS on Pixel hardware.
- Preconfigured, tested, and supported.
- Ready to use the day it arrives.
- Detailed Getting Started Guides.
- Detailed Migration Guides.
- Affordable.

Not a kit. Not a project. A phone.



Now, about the Ghost Phone we've been selling for four years. There are imposter companies that have come out selling something they also call the "Ghost Phone," ripping off our branding and trying to ride the coattails of what we've built. They're imposters. If you're not at mark37.com, it's not us. Unfortunately, some big names are now promoting one of these other entities thinking it's us. It's not us. What we actually do isn't a science project. We take GrapheneOS, which we support, and load it with a handful of applications to make your life easier, so you're not stuck asking, "Okay, I have the phone, now what's the safe mapping app? What should I use to open PDFs? What email app or browser should I use?" We have those preloaded, plus the documentation to get you up and running fast.

Telecom and the MVNOs

How Telecom Works

AT&T **T-Mobile** **Verizon**

MVNOs (Mobile Virtual Network Operators)

Cricket - TracFone - PureTalk
US Cellular - Patriot Mobile

All MVNOs ride on one, some or all of the Big 3 networks.
Your SIM card or eSIM in your phone
determines which network you're on.

MARK37.COM

On the telecom side, here's some knowledge. There are really only three carriers in the United States: AT&T, T-Mobile, and Verizon. Everyone else you've heard of, from Patriot Mobile to Cricket to Pure Talk to US Cellular, is a reseller, what's called a mobile virtual network operator, or MVNO. There are over 200 of them in the US alone. So the question isn't whether the phone will work with a given provider. The question is who owns the provider.

US Cellular, for example, is owned by AT&T. Pure Talk is a private company. Patriot Mobile is a private company. TracFone and Cricket are not private companies. If you've heard of Mint Mobile and wondered why their plans are so cheap, it's because they're selling your information to the carrier. Another thing to understand is that some MVNOs resell AT&T, some resell AT&T and Verizon, and some resell all three or a combination. So where you live also determines who the best provider is for you.

Your Carrier Sees Everything. Choose One That Doesn't Sell It.

AT&T, Verizon, and T-Mobile sell your location data. Legally. Regularly. To advertisers, data brokers, and government agencies.

The alternative: privacy-first MVNOs. Same towers. Same coverage. Different values.

PATRIOT MOBILE

Conservative values-driven carrier. No data selling, domestic customer service, and supports causes aligned with your beliefs.

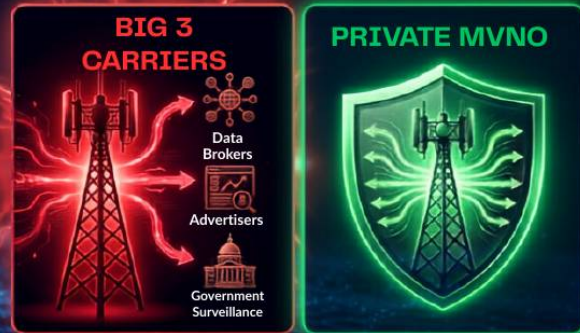
EFANI

Military-grade account security with SIM swap protection. Built for high-risk users who need bulletproof identity defense.

CAPE.CO

Near-zero data footprint. Minimal info required to activate, making you nearly impossible to hack or trace.

Full coverage. No surveillance.




We support a handful of companies we've vetted. One is Patriot Mobile, whose ads you've probably seen. They're good because they don't share your information. If they tell you AT&T has the best coverage in your area and put you on the AT&T network, fine. You're glad part of what you pay goes to candidates, causes, and organizations you support. They don't turn around and tell AT&T, "This new number belongs to this person, at this address, with this Social Security number and email." They simply tell AT&T they're activating and managing a new number on the line. That's far better than what most resellers do.

Understand that if you migrate your existing number to any provider, your track record comes with you, so people will still know that number was tied to you, and you may still get spam calls. If you get a new number, that doesn't mean you'll avoid spam either, because they're robo-dialing every conceivable number on the planet. People get frustrated, saying, "I just got a new number and I'm still getting spam." That's robo-dialing. They have no idea who you are, and they don't care.

Efani is a bit better from a security standpoint. They have military-grade account security, which makes it essentially impossible for someone to steal your number through a SIM swap. The downside is they're about 100 dollars a month. The upside is a 5-million-dollar insurance policy if someone does steal your information. If you use two-factor authentication for banking, crypto, and other important things, you may want to consider that as an insurance policy on your phone number. Cape.co is a newer company with a lot of funding and a different approach. They work somewhat like a VPN does for your laptop or phone, hiding who you are from the carriers and

making it very difficult to determine your identity. Do your own research, figure it out, and ask questions if you have them. That's what we're here for, on our live chat, at support@mark37.com, or through a free consultation.

Your Computer Is Watching You Too

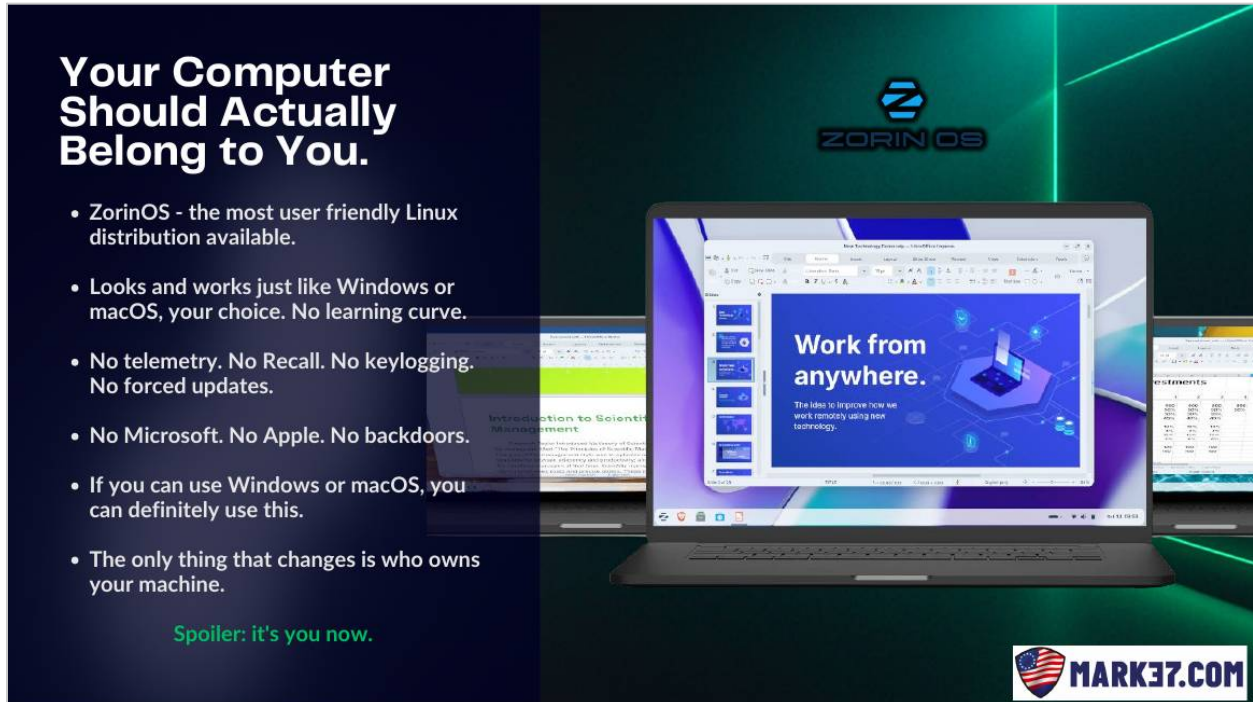


Your Computer Is Watching You Too.

- **Windows 11:**
 - Built-in keylogging.
 - Advertising IDs.
 - Telemetry that cannot be fully disabled.
- **Microsoft Recall:**
 - Screenshots of everything you do, every few seconds.
 - Stored in the cloud. Launched 2024.
 - Still shipping on new devices.
- **MacOS:**
 - Not much better. Still closed source.
 - Still tracks and monitors what you do.
 - Still reports home.



Your computer is watching you too, especially if you're running Windows. Windows makes it easy for us to sell digital privacy, because they're so egregious and in-your-face about what they're doing. It's as if they don't care anymore about hiding it. They've gone full throttle because they know the vast majority of people don't care, don't know, and don't want to know. And I hate to break it to the Mac users: Apple isn't much better. For everyone who's used Apple their whole life because it's so convenient, I'm telling you, the court cases prove definitively that they've been lying through their teeth. They're still collecting your information, still selling it, still using all of it to further lock you into a walled garden you can't easily leave.

An advertisement for ZorinOS. On the left, a dark blue panel contains the headline "Your Computer Should Actually Belong to You." followed by a list of six bullet points. The right side features a laptop displaying a desktop environment with a blue theme and a window titled "Work from anywhere." The ZorinOS logo is at the top center, and the MARK37.COM logo is at the bottom right.

Your Computer Should Actually Belong to You.

- ZorinOS - the most user friendly Linux distribution available.
- Looks and works just like Windows or macOS, your choice. No learning curve.
- No telemetry. No Recall. No keylogging. No forced updates.
- No Microsoft. No Apple. No backdoors.
- If you can use Windows or macOS, you can definitely use this.
- The only thing that changes is who owns your machine.

Spoiler: it's you now.

MARK37.COM

So here's a crazy idea: maybe your computer should actually belong to you. Maybe you shouldn't have to authenticate who you are just to turn on the laptop you bought and paid for. I know, I'm a crazy anti-technology terrorist for saying that. But that's what ZorinOS and other Linux operating systems offer. Your laptop becomes yours. We chose ZorinOS because it's the most user-friendly option out there. There are other good ones; I still run Pop!_OS, made by System76, on one of my laptops, and some of our people use Mint or Cinnamon. But Zorin is the friendliest, which is why we've standardized on it and preload it on the laptops we ship. My test is my 77-year-old dad, the least tech-savvy person on the planet. If I can put a device in front of him and he just uses it without calling me every day for support, I know it's good. Zorin can be made to look like Windows or like a Mac. You can toggle it to look, feel, and operate the way you want.

The Ghost Laptop

- ZorinOS pre-installed and configured.
- Private.
- Fast.
- Stable.
- Yours.



Not a project. A laptop.

*Can install Linux on YOUR current desktop or laptop!



So just as with the phone, all we're doing with laptops is taking ZorinOS and making it simpler to use. You can install Linux on a laptop yourself. It's a lot like installing a new engine in your car. You can do it from a YouTube video or a manual, but if you don't have someone next to you who's done it on that exact make and model, you're probably going to hurt yourself, mess up the car, or end up with a brick. So for those who want to dive in and figure it out, God love you, do it. But if you don't have the patience, time, or energy, we have a solution for you. And here's something huge: more people buying new laptops are now installing Linux than Windows. I never thought I'd see that day, but here we are. That's also why this is a game of whack-a-mole. As that happens, we're seeing increased efforts to lock things down even further.

You Don't Need Microsoft Office. You Never Did.

LibreOffice and OpenOffice are free, open-source replacements for the entire Microsoft Office suite.
...and they have existed for nearly 20 years!



What doesn't work: Microsoft's telemetry, forced cloud sync, and subscription fees.

Free. Forever. No Microsoft account required.



People ask how they'll open Word documents, spreadsheets, or PowerPoint. There's LibreOffice. It's open source and has been around for almost 20 years. Think about that: a free, open-source office suite that's been in the market for nearly two decades, which means you never have to pay Microsoft again. It opens and creates Word documents and Excel spreadsheets. The native file format is different, but they're interoperable; you can open and save as the Microsoft formats. People just don't know about it, because LibreOffice doesn't have billions of marketing dollars to convince you it's the better option. You can go to libreoffice.org, or openoffice.org, and install either one on your Mac or Windows machine today to get comfortable, because it's standardized on nearly every Linux machine.

Mic Locks, Faraday Bags, and Other Tools



Physical Security Hardware

MICROPHONE BLOCKERS
Physically blocks mic access.
3.5mm + Lightning + USB-C

SECURE CHARGERS
Charge without data transfer.
Blocks juice-jacking attacks.

FARADAY BAGS
Blocks ALL signals instantly.
WiFi, Bluetooth, Cellular, GPS.

...also available at MARK37.COM



Some of you have heard of mic locks, or mic blockers. We sell those on our website, and they're really cool. This tiny little dongle plugs right into your phone. As far as your phone is concerned, it becomes the new microphone. It sends a null signal into the phone, so the phone can't listen to everything happening around you, because it thinks this little plug is the microphone. The Lightning version, for older iPhones, runs about 30 dollars. The USB-C version, for newer iPhones and Android devices, is about 20 dollars. Dirt cheap, and it solves the problem of your phone listening all the time. It should be a no-brainer.

Here's a personal story that's heart-wrenching for me and for my daughter. When she was 13 or 14, she was flashing phones with me. I taught her how. We ran this business out of my home office and our garage. At events, customers would come up to our booth and we'd give them a condensed version of everything I'm telling you now. They'd say, "Yes, I'm so tired of my phone spying on me." I'd say, "Great, here's a mic lock for 20 bucks that prevents it from listening." And they'd say, "Oh, that's a little steep, I don't know if we have 20 bucks for that right now, we'll get back to you." Then they'd walk to the booth next to us, which was selling flavored pork rinds, and spend 100 dollars on pork rinds. My daughter would look at me and ask, "What is wrong with people?" And I'd throw my hands up and say, "I don't know, honey. We live in clown world."

We carry other things too: secure chargers and Faraday bags. A secure charger prevents someone from stealing the data off your phone when you plug in to charge. This is spyware the CIA and

intelligence agencies used 15 years ago at great cost, and now it's a 10-dollar item you toss in your backpack. Just as it's gotten easier and cheaper for us to protect ourselves, it's gotten easier and cheaper for bad actors to spy on us, to put tiny cameras all over Airbnbs, VRBOs, and hotel rooms that people don't know how to check for. We at least have to be aware this is happening.

Faraday bags are important, but a lot of people think that throwing their phone in one solves everything. It doesn't. If your phone is in a Faraday bag, it can still record the conversation around you and you talking, and it will wait until you pull it out to transmit everything it recorded. So a Faraday bag doesn't solve the listening problem on its own. The good news is that if you're running GrapheneOS, your phone isn't listening unless you tell it to, because you now control the phone. You decide what happens on it.

Swapping Apps

Swapping Apps Takes One Saturday Afternoon.

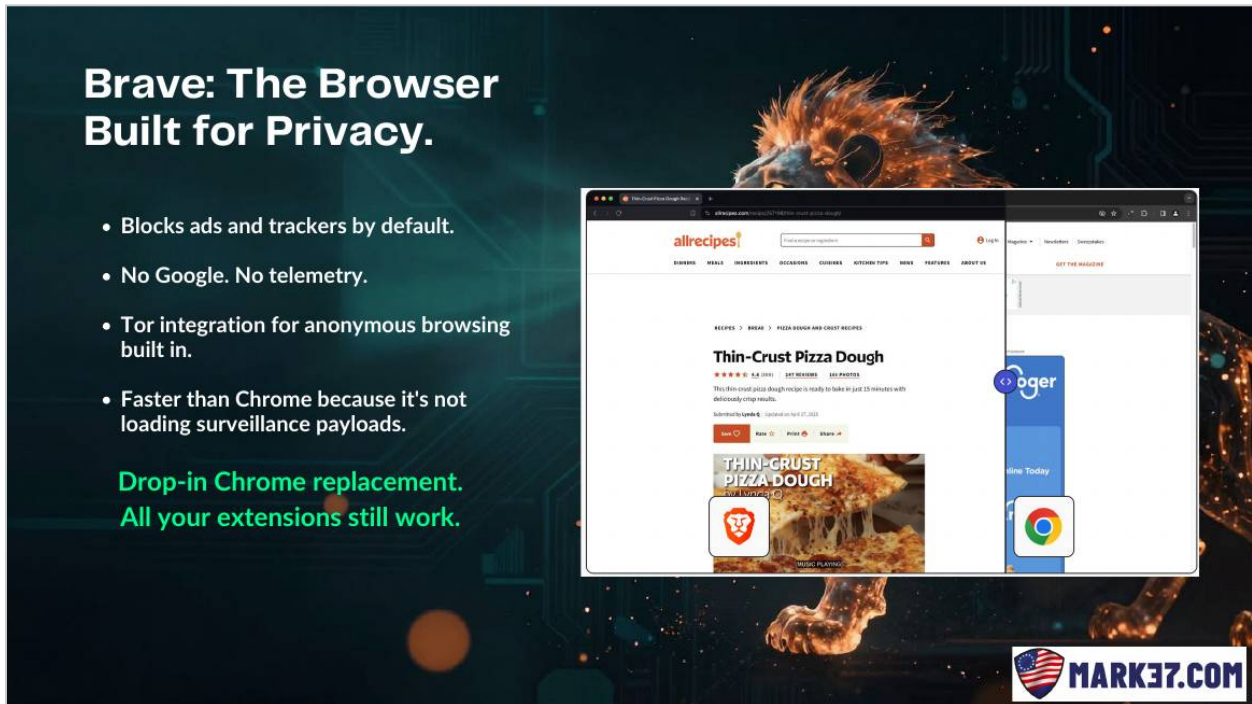
DITCH THIS	REPLACE WITH	TIME
Gmail / Yahoo / AOL / Outlook	StartMail / Thunderbird	30 - 60 min
Chrome / Safari	Brave Browser / Vanadium	5 min
Google Search	Brave Search	1 min
iMessage / Google Messages	SMS / MMS	15 min
Google Maps / Waze	CoMaps / Magic Earth / OSMAnd+	15 min
WhatsApp	Signal / Session	15 min
Google Drive / iCloud	Ente Photos / Immich / Nextcloud	60-90 min



Swapping apps takes an afternoon at most. The thing that takes longest is migrating a ton of email, or a lot of photos and videos. The rest you can whiz right through, because there are so many alternatives. Vanadium is the stock browser on a GrapheneOS phone, and it's great. Brave is a great browser, and Brave Search is great; you can even use Brave Search inside Vanadium. People ask about DuckDuckGo. I hate to break it to you, but I don't trust DuckDuckGo. They lied from the beginning about how they delivered their service, using Microsoft Bing on the back end while claiming it was their own. They were faking it until they could make it, so they lost all credibility

with me.

You can migrate your SMS texts over and use different messaging and mapping apps. Waze, by the way, is owned by Google, so when people say they use Waze, that's Google. There are other mapping apps. Are they all perfect? No, but they're getting better, and the more people use them, the better they get. They just haven't had trillions of dollars and decades of development. The good news is that building software gets easier, simpler, and cheaper every day, so these tools improve daily. WhatsApp is owned by Facebook, another company lying to you when it says all your data is encrypted and they have no access. They do have access. For Google Drive and iCloud, there are all kinds of alternatives, and we're constantly working on migration software to move your stuff out faster, along with our own software and services to help.



Brave: The Browser Built for Privacy.

- Blocks ads and trackers by default.
- No Google. No telemetry.
- Tor integration for anonymous browsing built in.
- Faster than Chrome because it's not loading surveillance payloads.

Drop-in Chrome replacement.
All your extensions still work.

MARK37.COM

Something as simple as Brave, built for privacy from day one, means you won't see ads on the vast majority of sites you'd otherwise see on Chrome, and the sites you visit aren't being tracked on the back end and fed to companies like Amazon or Facebook.


Meshtastic, Blackout Comms, and Ghost Home

What Happens When the Internet Goes Away?

Two proven options. Same mission. Different approach.

MESHTASTIC + LilyGO RNode


- Open source. Phone-paired. Community mesh.
- Encrypted LoRa radio messaging.
- 2-5 mile range per node.
- Unlimited range with enough relay nodes in the field.
- Works with GrapheneOS. @ \$75/node.
- No cell towers. No internet. No carrier.
- Best for: community mesh networks, neighborhood resilience, tech-comfortable users.



FOSS - free and open source.


BLACKOUT COMMS

- Stand alone device - no phone required.
- Runs on LilyGO T-Deck, Pager or Touchscreen / keyboard interface.
- Frequency hopping for anti-jamming.
- Private clusters. Stealth modes.
- MeshCore network mixing - auto-switches between mesh systems for maximum range.
- Best for: operational security, grid-down scenarios, phone-independent comms.



Proprietary firmware, licensed.

Both: encrypted, off-grid, no carrier, no internet required.



Here's some fun stuff. There's something called Meshtastic. I live in upstate South Carolina. Remember Hurricane Helene? I lost about 20 trees on my property, and we were out of power, internet, and phone service for two weeks. It was nuts. Thankfully I had a bunch of LilyGO devices running Meshtastic, and I'd trained my neighbors on how to use them, so we could still communicate when everything else was down. You can create a decentralized, encrypted mesh network with these devices to communicate with people in your neighborhood. The limiting factor is range, only about two to five miles.

Blackout Comms is similar. The difference is that with Meshtastic, the software runs on your phone and a separate walkie-talkie-style device feeds the signal to it, whereas with Blackout Comms it all happens on the device itself; the device is the communicator. These tools exist, folks. People just don't know about them, and we need more people using them so developers can make them better. I think Meshtastic is better for local community. Ham radio is good for much broader range, but you have to be licensed, and it clears through towers controlled by the FCC. These mesh tools aren't controlled by the FCC at all.

Home Intelligence That Actually Works for You.

Ghost Home is a fully sovereign home intelligence platform.
It runs locally on hardware you own.

The AI that talks to you, listens to you, and helps you manage your home never phones home -
because it already is home.

Built on Home Assistant and powered by a based local large language model,
Ghost Home gives you a genuinely intelligent home that you actually own.

Talk to your home in plain language. It responds.
Monitor your router and network health in real time.
Manage connected devices and cameras without a corporate app or account.

Your data stays on your hardware. Full stop.
Works without internet. No cloud dependency. Ever.

CLOUD AI

Your Home
↓ ↓ ↓
OpenAI / Google / Microsoft / Amazon
Your data leaves. Forever.

GHOST HOME AI

Your Home
contained
All AI runs locally. Nothing leaves.
Yours.



One thing we're really excited to roll out is Ghost Home. It runs in your home on an open-source home-automation platform called Home Assistant. You can go check out Home Assistant right now. The tools are great, but they're currently in a place where you have to be a developer and a tinkerer to get everything working. So, just like the phone and laptop, all we're doing is taking the existing tools and packaging them so anyone can use them, so I can hand it to my dad and not get constant tech-support calls.

The other cool thing about Home Assistant is that we're tying it to your own local large language model, your own local AI, which means it's not owned by Anthropic, Google, OpenAI, or anyone else. You own it. You control it. You train it. It will only reach outside your home network if you give it access and if you tell it to. If you don't tell it to, it won't, because you own it. You're the master. My super-geek friends have already built these and run them in their homes, but it took them 10 hours or even days to set up. That's not accessible. We need to make it accessible. We're hoping to roll this out in July, so stay tuned and sign up for our newsletter. If you've ever seen Iron Man, this is like having JARVIS, his home AI, serving you, helping you make sense of what's happening around you and protecting your home network. Because anyone who tells you to just buy this router and you're safe is lying. You have to learn how the router works and how to set it up. This home AI system will be able to talk to it, understand it, coach you through setup, and then monitor it to make sure nothing crazy is going on. That's pretty cool.

A Journey, Not a Sprint



As I keep saying, this is a journey, not a sprint, and we have tools to coach you through it. You start with basic awareness, which you've been doing with me for the last hour and a half. Thank you to everyone who's stayed. It gives me hope in humanity that people are taking this seriously. Then you move through the process. Do the audit. You're aware now, you can't unlearn what I've taught you, so you have to do something. Go to the Start Here link, download the roadmap, and start working through the checkboxes. You'll get there.



Your Geek Squad for Sovereign Tech.

- Ghost Phone. Ghost Laptop. Ghost Home.
- Sovereign carrier partners.
- App setup and migration support.
- Ongoing tech support by people who actually believe in this.



We don't just sell you a product. We make sure it works.

We serve as your geek squad for sovereign tech. That's our whole existence. It started as us scratching our own itch, wanting these tools for ourselves, and then packaging them so they're accessible to everyone.

We fought the battle over COVID. Now we have to fight digital ID and the battle for the digital domain. If you understand how this operates, this is the last frontier before we go full totalitarian, China-style. We have to fight it. At this point we have thousands of customers on the other side of this who are deeply thankful. On our consultation calls, we pray with people regularly. We ask whether they're in the Word, and if they don't have a Bible, we'll send them one. That's the most important thing for us as a business. We use this business as a ministry and a way to preach the gospel, because we need people awake. You can't be on the front lines of this war without realizing that your relationship with your Creator is the most important thing in your life. If you don't have that figured out, none of the rest matters.

The Most Important Device in Your House Belongs to Your Kid(s).

Social media algorithms were engineered by teams of behavioral scientists and psychologists to maximize time-on-app.

The research on adolescent mental health is not ambiguous. The platforms know. The internal documents prove it.

There are various functional "smart" and "dumb" devices that already solve for this.

They can call, text, take photos, and use apps.

What they can't do is be groomed by platforms built to addict them.

You can give your kids the tools without handing them to the machine.



And remember, the most important devices in your house are the ones that belong to your kids. We cannot keep giving children access to the most addictive things ever designed, things built to pull them into content they shouldn't see even as adults. That's what these are designed to do, and there are options.

Cash is not dead. But your window is closing.

Programmable Money

- CBDC pilots are live in over 100 countries.
- The BIS - the central bank of central banks - has published its framework for programmable money.
- Programmable money can be restricted by category, time, behavior, or compliance status.
- This is not theoretical. It is a published policy goal.

Sovereign Finance

- Hard assets. Precious metals.
- Bitcoin in self-custody - not on an exchange.
- Cash, while it still works.
- Local trade relationships.
- Bartering
- Parallel financial rails.



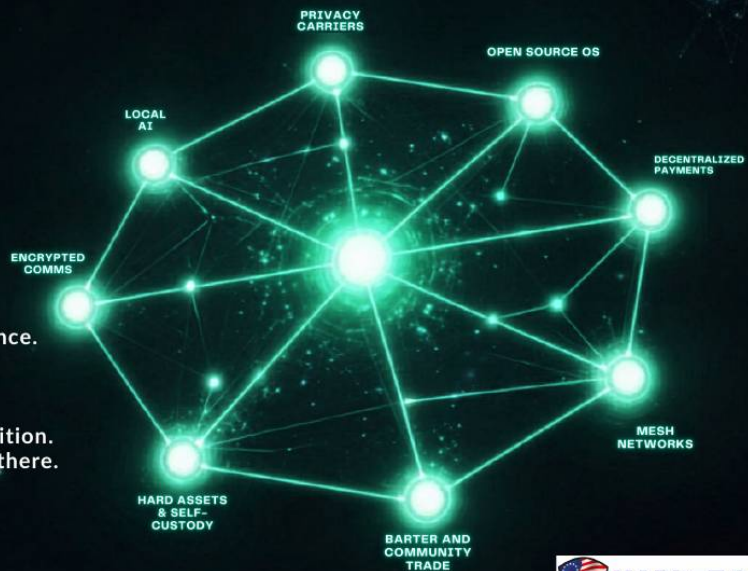
Realize too that cash is not dead, and the window is closing. A lot of people own silver and gold, but when I ask whether they've ever actually used it to buy, sell, or trade something, they say no. Get comfortable doing that. The dollar should not be the only thing we use as a means of energy transfer, because that's all money is, a means of energy transfer. Get comfortable trading time for services, or chickens for eggs, or eggs for meat. I now make a point to do a different kind of non-dollar transaction every week, because the time is coming when they'll say that to use the internet or participate in the new global economy, you have to convert your money into a central bank digital currency. The administration says it's fighting CBDCs, but I watch actions, not words, and on the back end they're building all the infrastructure for it.

THE PARALLEL ECONOMY

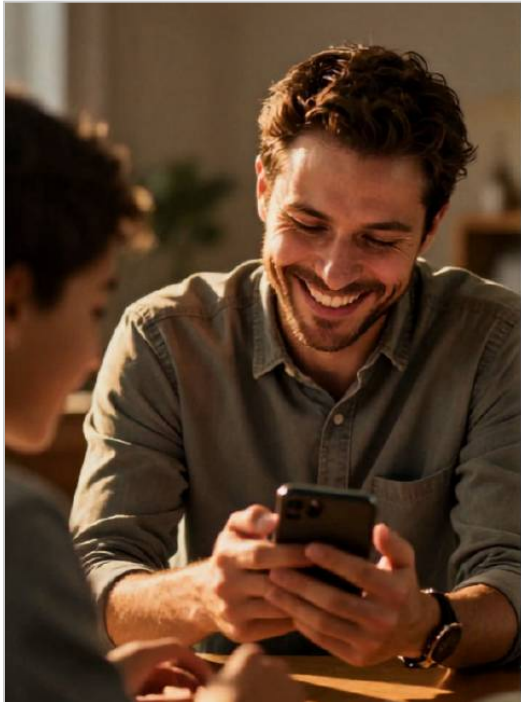
Alternative Infrastructure Already Exists.

- Privacy-first carriers.
- Open source operating systems.
- Encrypted communications.
- Decentralized payment rails.
- Local AI.
- Mesh networks.
- Hard assets and self-custody finance.
- Community trade relationships.

None of this is fringe anymore.
Tens of millions have made this transition.
The tools are mature. The support is there.



Get involved locally. Get to know your neighbors and build your community. You're not alone. We have a whole community online and offline, including groups we call Ghost Teams assembling in different areas to build community among people who understand how important this is and want to spread awareness. We have an article in the resources section of our website that points to at least 40 organizations around the country that can connect you with people thinking along the same lines. You can engage with us on Telegram, Rumble, and X, at support@mark37.com, on our live chat, or by booking a free consultation. We have a great Telegram community, with people who've been there for years and can answer your questions.



YOU WON'T DO THIS ALONE.

MARK37 exists because you shouldn't have to figure this out yourself.

Beyond the products there is a growing community of people who have made this decision and are living it.

Real people. Available.

Not a forum thread. A community.

Find us.


support@mark37.com

LiveChat via [MARK37.com](#)

Telegram:
<https://t.me/MARK37public>

Rumble:
<https://rumble.com/mark37>

X:
https://x.com/MARK37_com



Once you've gone through this process, the anxiety on the front end gives way to feeling so much better on the back end. It's like eating a steak from a cow you know was raised properly, from a farmer you know. It tastes exponentially better than the stuff you bought at Costco or Food Lion or Piggly Wiggly. You'll feel that much better on the other side of this.

YOUR LIFE ON THE OTHER SIDE

You Wake Up. Your Phone Doesn't Know Who or Where You Are.

TODAY

GHOST LIFE

Your email provider doesn't read your communications. Your laptop doesn't take screenshots of your work.
 Your search history isn't being profiled. Your AI assistant doesn't report back to a server farm in Virginia.
 Your carrier doesn't sell your location data.

You still have fast internet. You still use apps. You still bank online. You still connect.
 You just do it without being surveilled and sold 24 hours a day.

That's not a sacrifice. That's a restoration.

What Does Digital Sovereignty Feel Like?

It Feels Like Quiet.

- No background hum of being watched.
- No wondering what that ad knows about you.
- No feeding a machine that is being built to control you.
- You own your tools.
- You own your data.
- You run your life.

It feels like what normal used to be.
Before we handed it away.

I love this Buckminster Fuller quote: you never change things by fighting the existing reality; to change something, build a new model that makes the existing model obsolete. We have to reclaim our culture, and we can do it together. We just need the tools. We have to stop using the tools of the enemy to fight the enemy, and start using tools designed to serve us.

**"You never change things by fighting
the existing reality. To change something,
build a new model that makes the
existing model obsolete."**

- Buckminster Fuller



And because I'm a big Star Wars buff, here's my Yoda: do or do not, there is no "think on it." I can't tell you how many times I've heard people say, "This all makes perfect sense, I'll think on it," and then do nothing. We have to take action.

Ditch BigTech You Must

**Do... or do not.
There is no "think on it"**



There's no more time for talk and no more excuses. Make a decision today. Start the roadmap. Book a consultation, get a mic lock, do something. Stick to it. Step by step. You've got this.

ONE DECISION. TODAY.

You don't have to do everything at once. Start with one thing.

01
DOWNLOAD THE ROADMAP
Replace your browser.
Takes minutes. Free.

02
GHOST PHONE OR LAPTOP
Order online.
Pre-configured. Ready to go.

03
JOIN + BOOK A CONSULT
Email list. Free 30-min call.
We'll map your path.

One step. Then the next. We'll be here.

MARK37.COM

That's the presentation. Let me dig into the Q&A for those of you still with us, which is most of you. That's awesome.

Q&A

From Craig: For banking, I'm required to use Symantec VIP Access for two-factor authentication. Can I use this on a Ghost Phone without compromising privacy?

Yes, Craig, you can. There are several third-party 2FA apps. A lot of people think they have to use the Google authenticator. You don't; there are plenty of other authenticator apps you can use.

On the privacy and security piece, people often ask, "If I'm using a Ghost Phone and the person I'm talking to is on an iPhone, are our communications still secure?" Think about it logically. If they're still on an iPhone, that operating system is going to see the conversation on their end. It's like using an encrypted email app to email someone with a Gmail account: Google still gets that email. That's why we need to spread awareness and get more people using these tools. There's also a concept of living in the public versus living in the private. I have devices I know will be shared in the public, and I have devices, phone numbers, and email addresses I only use in the private, with people I know take their privacy seriously. That's advanced-level stuff, for someone like me who travels

and preaches this message, so my level of privacy is different from most.

What about YouTube?

YouTube will still track you, but there are alternative apps that let you watch YouTube videos without YouTube knowing who you are or what you're watching. That's the cool thing: for nearly every "what about this app" question, there's an alternative. One is called Grayjay; look it up. Another is NewPipe. We preinstall those on the phones so you don't have to start asking which is best. That list evolves over time. We used to install about 40 apps on the phone, and half of those we no longer install, some because the developer community stopped supporting them and we don't know what holes might be in them, some because they got bought by corporations and started tracking, and some because there are simply better alternatives now. On our website we constantly update which apps we preload and explain exactly what each one does.

Can you recommend a landline for phone communications?

Unfortunately, there's really no such thing as a traditional landline anymore. Your local carrier might sell you a phone line, but that line is actually running over fiber or cable, over the internet, at the end of the day. There are companies that will sell you a rotary phone you can connect, but understand it's running as voice over IP over the internet, not over the old-school telecom infrastructure.

From Terry: Do these systems also track stored text messages on my iPhone?

Yes, hands down. If you have an iPhone, Apple is tracking and storing all of it. In fact, it's not even living only on your phone; it's living on their servers. That's why the whole communications platform is controlled by Apple, or Google. You're clearing all of your calls and texts through their servers. We have articles that break this down in plain language. My test, again, is my dad: if he can't read an article and understand it, I know we have to do better. The articles on our website are written for people who aren't tech savvy. So, Terry, read the articles, get educated, and when you're ready, sign up for a consultation and we'll walk through your questions.

Thank you, and God bless you. Thank you so much for giving me almost two hours of your time. I hope this was helpful and useful. If you have feedback about something I missed or could have done better, I'm always open to it. Feedback is a gift. You can reach me directly at sean@mark37.com. Please reach out, and send any questions to support@mark37.com. I promise we'll get back to all of them. Thank you again for your support and your prayers. Please pray for us. We only exist because of the prayer warriors around the country praying for us regularly. Thank you so much. God bless you all.



MARK37.COM

Your Geek Squad for Sovereign Tech.

FREE 30 MINUTE DIGITAL PRIVACY CONSULTATION

www.MARK37.com

SUPPORT@MARK37.COM

Live Chat: MARK37.COM | 9am-5pm Mon-Fri