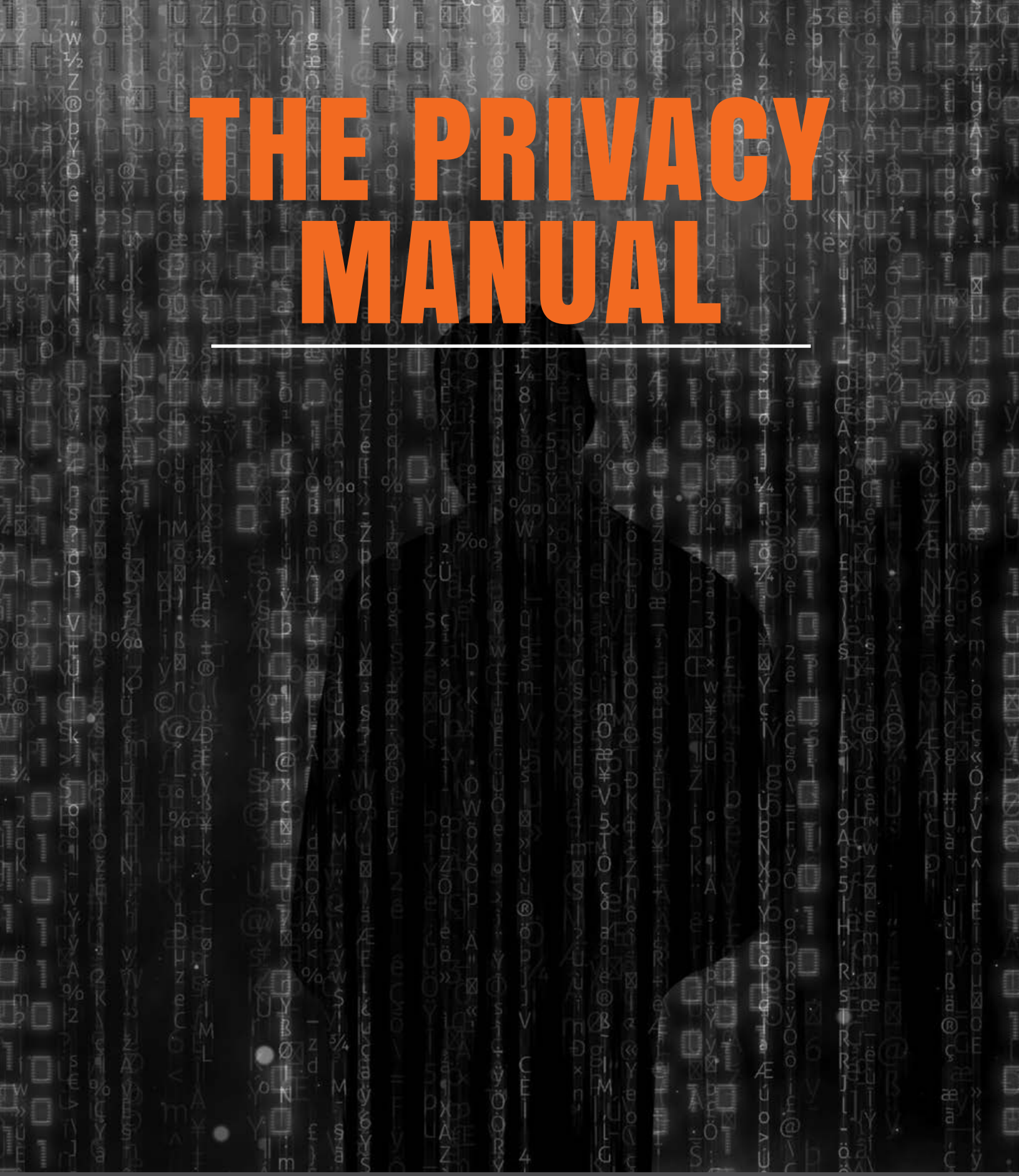
THE PRIVACY MANUAL



BY INTERNATIONAL LIVING

INTERNATIONALLIVING.COM

The Privacy Manual

An *International Living* Report

Cover photo: ©pixabay.com/tigerlily713

TABLE OF CONTENTS

“If you’re serious about protecting and preserving your family’s wealth, you can’t afford not to read this report.”

—Jackie Flynn

INTRODUCTION

Last year, almost 4 million people became victims of identity theft in the U.S., more than double the figure from 2019. The amount stolen reached $43 billion.

And those numbers don't include the exponentially larger numbers of people whose personal information has been exposed due to lax security by companies holding your data…data that can be used to steal your identity.

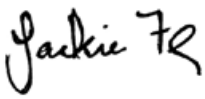
Protecting your privacy online has never been more important.

That's why the information contained in this report is so vital. Within its pages our experts reveal:

- How to put a freeze on identity thieves.
- If you've ever borrowed money or applied for a credit card, then your data is likely at risk. Turn to page 3 to discover what you can do about it.
- How to make your Bitcoin invisible (and off the grid). See page 6 for more.
- Do you use the WiFi at hotels, offices, or even your home? Then you need this easy-to-use tool to protect your online privacy. (You can even use it to stream free TV and unlock hidden shows on the streaming platforms you use). Find out what it is and how to get set up on page 13.

If you're serious about protecting and preserving your family's wealth, you can't afford not to read this report.

Sincerely,



Jackie Flynn,

Publisher,

International Living

How to Put a Freeze on Identity Thieves

By Mark Nestmann

The only solution to defend yourself from identity theft is to put a security freeze on your credit files.

In the old days, thieves had to come in, guns blazing, and threaten or commit acts of violence to take what you'd earned from you. At the very least, they had to cut a very noticeable hole in the vault wall to access your bank account.

These days, it's far more sophisticated, and the tracks are far more difficult to see. Your bank accounts, credit rating, and reputation can be left in ruin without your ever knowing you've been attacked.

In 2020, almost 4 million people became victims of identity theft in the U.S., more than double the figure from 2019. The amount stolen reached $43 billion. But those numbers don't include the exponentially larger numbers of people whose

personal information has been exposed due to lax security by companies holding your data…data which can be used to steal your identity.

For instance, in 2017, Equifax had virtually its entire database of consumer credit reports—nearly 148 million in all—stolen by hackers. The attack occurred because Equifax failed to patch a software vulnerability it had known about months before the breach occurred.

If you've ever borrowed money or applied for a credit card, there's an Equifax file with your name on it. And thanks to the company's depraved indifference to online security, the hackers that stole its database have access to all the data necessary to steal your identity:

- Your Social Security number
- Your date of birth
- Your home address

Your data could be sold to allow someone else to open bank accounts in your name, borrow money…even apply for a passport.

Consider what happened to Paul Little, a native-born U.S. citizen, when he applied for a passport. He got turned down, even after presenting his birth certificate, driver's license, Social Security card, baptismal certificate, school records, tax returns, his parents' death certificates…even a copy of his high school yearbook.

Little eventually learned that he was an identity theft victim. Someone impersonating him had already obtained a passport in his name.

How can you protect yourself from the consequences of identity theft? There's only one reliable way to do it: a security freeze on your files at Equifax and the other major credit bureaus.

A security freeze, in effect, places an electronic padlock on your credit report. Only your existing creditors (credit card companies, mortgage issuers, etc.) can review your credit report until you remove the padlock.

If an identity thief tries to apply for credit in your name, he'll be in for a rude surprise. That's because if a company can't review your credit report, it's very unlikely to issue you (or an imposter) credit.

In other words, a security freeze eliminates identity theft at its source—the ability of a criminal to obtain credit fraudulently.

For instance, let's say an identity thief buys data stolen from Equifax or another source (there are many) that includes your name, address, birthday, and Social Security number.

Next, the thief uses this information to obtain a driver's license or other official document containing your name, but the thief 's photo. Finally, he visits a car dealership or other seller of "big-ticket" items.

Say he test drives a luxury car and tells the salesman to "charge it"—to you. With a credit freeze, the thief 's application for credit in your name will be turned down. Without a credit freeze, he might drive off in a new car, leaving you to pay the bill.

Security freezes are authorized in all 50 states. If someone fraudulently accesses your credit report despite the freeze, you're protected from financial liability.

You'll need to put a security freeze into effect with each major credit agency. See:

- Equifax: *https://www.equifax.com/personal/credit-report-services/credit-freeze/*
- Experian: *Experian.com/freeze/center.html*
- TransUnion: *https://www.transunion.com/solution/customer-acquisition*
- Innovis: call: *1-800-540-2505*

Credit bureaus hate security freezes, because freezing and unfreezing accounts often requires the intervention of a customer service agent. In addition, they can no longer sell your data to companies that might want to offer you credit and other products or services.

Instead, credit bureaus will try to persuade you to sign up for a "credit lock" and credit monitoring services. Essentially, you pay a monthly or annual fee (which is often waived) for the privilege of having the company who should be keeping your data safe notify you when they don't.

Don't be fooled. A credit lock is only an agreement between you and the credit bureau. You're bound by the restrictions in the fine print of the agreement, rather than by your state's security freeze law.

There is little incentive for banks, credit bureaus, email services, and other data repositories to invest in security. Your personal data is a product to be bought and sold, and any limits to this practice cut into their profits.

The only solution to defend yourself from identity theft is to put a security freeze on your credit files.

Privacy Coins: How to Buy and Sell Cryptocurrencies Anonymously

By Jeff D. Opdyke

©Istockphoto.com/turk_stock_photographer

Tracking the wallet address on privacy coins is hard, if not impossible.

Money launderers. Drug dealers. Hackers. No doubt, these are the people you envision when you hear experts claiming that bitcoin—because it's supposedly anonymous—is the playground of the world's scoundrels.

But the thing is, that's not accurate.

Bitcoin's purported privacy isn't all it's cracked up to be. Frankly, it's easier to launder physical dollars than it is to launder bitcoin. That's because every single bitcoin transaction exists in digital form, on the blockchain, and the data behind that is visible to anyone who cares to look.

Now, to be clear, personal information like your Social Security number, address, phone number, etc. is not visible through the blockchain. But transaction data is, meaning that governments and even ordinary folks on the internet might be able to determine that you own bitcoin.

That's not to say, however, that cryptocurrency can't be a private affair. It can—if you know what you're doing.

So, here's what you need to know if owning and trading cryptocurrencies privately is high on your agenda.

Is bitcoin anonymous?

In the early years of bitcoin, the media liked to report on bitcoin's privacy. Journalists often suggested that owners of bitcoin were unknowable because bitcoin trades on the blockchain as long strings of letters and numbers that look like this:

1DxAmdLeOfaBCTco1NADr3sSVdsf5ts6hd

That's what's known as a "bitcoin wallet address" and it does seem pretty private. Who has any idea where that string of gibberish leads? Only, it's not really private at all.

That string of gibberish is forever locked onto the blockchain—a shared ledger of all the transactions that have ever occurred. And in certain circumstances, the address can be traced directly back to the person who uses it.

For instance, let's say I am the owner of that bitcoin address at a crypto exchange such as Coinbase. And let's say the Internal Revenue Service subpoenas Coinbase, demanding information on all account holders. And let's say Coinbase submits to IRS pressure (which is exactly what Coinbase did in 2018).

What that means is the IRS now knows that bitcoin address is attached to me.

Which means the IRS could search the entire blockchain for that address and see exactly what I did with my bitcoin. It would be able to see how many bitcoins I deposited into that address, how much I sold out of that address, and where I spent my bitcoin (assuming I used that wallet as the source of spending).

Moreover, it could track all the addresses to which I sent my bitcoin, and then all the addresses that spring off from there. In effect, then, bitcoin and the blockchain are the absolute perfect paper trail because they are permanent and unchangeable. It's one reason government actually likes blockchain: It can track the movement of money.

Frankly, it's like that with just about every cryptocurrency on the planet. Though the wallet addresses say nothing overtly about the owner, behind those numbers and letters are pretty much everything government authorities and regulators need to know in order to track you down.

But notice my language: "just about every cryptocurrency on the planet."

I specifically chose that phrasing because not all cryptos are so visible.

There is a small group of cryptocurrencies known as "privacy coins," and they are exactly what their name suggests.

How privacy coins work

Privacy coins are not dramatically different than bitcoin in that they exist on the blockchain.

So, transactions are visible. However, tracking the wallet address is much harder, if not impossible. There are different strategies that cryptocurrencies use to accomplish this. One is stealth addresses.

Certain privacy coins create a new address each time a transaction occurs. An outside observer would not be able to tell what occurred in the transaction or the real wallet addresses involved. That makes it impossible to track that crypto. And because the address goes away and is never seen again, it's impossible to then "follow the money."

That's a privacy coin.

Critics claim that privacy coins should be illegal. That's as logical as saying cash should be illegal. Cash is exceedingly private. The government has no clue where you spend cash. Technically, it has no clue where you earn cash outside of your paycheck. Or where you hide cash. Physical currency is a deeply private form of money.

Why should crypto be any different just because it's electronic?

Nevertheless, governments are increasingly leery of crypto privacy because they want to know where you earn and spend your money. They want to be able to track it. They claim that's to thwart crime.

There's some truth to that—though there's an equal amount of truth to the idea that government simply wants an easy way to snoop on its citizens' financial lives.

This is going to become an even-more pressing topic as central banks launch digital fiat currencies. Already, China has released a digital yuan. Europe is working on a digital euro. And the Federal Reserve has publicly stated that a digital dollar is in America's near future.

Those will all work with digital wallets connected to the government. Thus, earnings and spending will be directly visible by the government. In that world, people will absolutely seek out some form of digital privacy when it comes to saving and spending.

That's where privacy coins are going to shine.

Can I keep my bitcoin private?

There are ways to keep bitcoin private, too, even though it's not a privacy coin.

There are services that offer to increase the privacy of cryptocurrency transactions. They do this through a variety of processes. One is through pooling transactions so that individual transactions are harder to identify.

That's what Wasabi Wallet does. Wasabi is a highly regarded crypto wallet that pools smaller transactions into a single, larger transaction with multiple inputs and multiple outputs.

The result means that an outside observer would not be able to determine the original sources of that larger transaction. Nor would they see the wallets to which all the bitcoins were distributed.

With such a service, you could buy bitcoin privately, transfer it to a "cold wallet"—one that is not connected to the internet—and your bitcoin would be entirely off the grid and out of view, from initial transaction to storage.

What are the primary privacy coins?

If you want to own privacy coins directly, there are several to choose from.

The big two are **Monero (symbol: XMR)** and **Zcash (ZEC)**. They suck up most of the oxygen in the world of privacy coins. Investors have put about $3.7 billion into Monero, and nearly $1.4 billion into Zcash. (The next biggest player is just one-third the size of Zcash.)

Each operates differently to accomplish the same end: privacy.

Though Monero is bigger, I'd opt for Zcash if you want to own a privacy coin.

Here's why: Governments are wary of privacy coins. Already, some crypto exchanges are so worried about a government crackdown that they have preemptively delisted Monero. Some have delisted Zcash, as well.

The reality, of course, is that government has little chance of fully banning any cryptocurrency. They'd have to effectively shut down the internet since there are so many ways of trading privately, such as through Virtual Private Networks (VPNs) or privacy browsers like TOR.

Still, if governments were to ever crack down on privacy coins and try to ban them, both Monero and Zcash would feel the brunt (as would all privacy coins).

But Zcash would be less impacted.

That's because Monero is purely a privacy coin, while Zcash transactions can be private or public.

Zcash is a direct spin-off of bitcoin. It is essentially bitcoin with a privacy overlay. As such, if I wanted to send Zcash to you, we can conduct that transaction in one of four different ways, depending on the level of privacy we need:

1. Totally private.
2. Totally transparent.
3. My address private; your address transparent.
4. My address transparent; your address private.

Those options, I believe, will serve Zcash well in a world where governments come down on privacy coins. Zcash can legitimately make the argument that it is not purely a privacy coin.

That helps explain why Zcash is the number two privacy coin, and why its price over the last year has moved from about $37 to around $128, as I write this (and it has been as high as $350 in the past year).

You will find Zcash available on many U.S.-based crypto exchanges, including my recommended exchange, Binance.US. However, Binance.US is not available in all U.S. states. If you live in Texas or New York, for example, then you should look to Gemini.

The wrap up

Ultimately, the big question here is whether privacy coins make sense.

And the answer is yes, they certainly do.

There are many reasons someone might want privacy in their spending that have nothing to do with criminality, such as buying medical goods online or putting assets out of the reach of creditors. Transacting privately through the blockchain can allow this.

Frankly, however, I would rather own a privacy coin such as Zcash instead of going through the process of mixing and privatizing bitcoin with a wallet like Wasabi. Those mixing and privatizing services impose a fee.

It's easier to just own a privacy coin directly since the trading fees are minimal.

However you approach it, privacy coins face a choppy future until governments decide how they will approach these assets. But don't let that put you off. Privacy on the blockchain is going to become increasingly important once global central banks give us digital currencies.

How to Protect Your Privacy Online

By Jeff D. Opdyke

Istockphoto.com/anilakkus

Always use a virtual private network, or VPN, on public WiFi to protect your online privacy.

In my many years traveling the globe, I couldn't begin to estimate the number of times I've sat in an airport lounge or in a café or on a hotel bed and logged into the public WiFi to check my email or my freelance-writing accounts or whatever.

As it turns out, that was pretty unwise…potentially downright dangerous. Or at least, so says the FBI. In recent years, the bureau has frequently warned about the dangers of using public WiFi.

One of the most recent of these announcements cautioned specifically about the perils of using hotel wireless networks. The problem with hotel networks—indeed public WiFi in general—is that they are built for convenience, not security, which has made them a preferred target for hackers.

Hotel owners' primary objective is not to make networks secure, but to stop angry tourists calling the front desk because they can't figure out how to get YouTube working on little Jimmy's iPad.

This means they often leave their WiFi networks wide open, so anyone can log on whenever they want. Or they have the password written in a prominent public place, or use a basic access system such as a combination of room number and password.

However, if you find it incredibly easy to access the WiFi, so will nefarious actors. Using these open networks, the FBI advised, could allow hackers to gain access to your browsing history or redirect you to fake log-in pages, where you might input some crucial information, like your company email password, because you believed you were on the official site.

With your work email and password, cyber-attackers could gain access to your company network and start hoovering up corporate secrets or implant ransomware—a form of malicious software that blocks access to files unless a ransom is paid.

Then there's the possibility of an "evil twin attack." This is where the hacker has actually set up the open WiFi network you're accessing. I mean, think about it. When we're looking for public WiFi in a hotel or an airport, we generally just open our phones and click on the one that's got a correct-sounding name and a strong signal.

Thing is, if we log on to a network operated by a hacker, we might as well just hand them over the keys to our digital lives. The solution, according to the FBI, is to always use a virtual private network, or VPN, on public WiFi.

The online tool you need to have

I first started using a VPN in the mid-2000s. Today, I basically never use the internet without having one turned on…no matter if I'm on public WiFi, on my home internet network, or using 4G on my iPhone. There are several reasons I always use a VPN when online:

First, security and privacy. Even on home WiFi networks, which are generally pretty secure from hackers, VPNs are an effective way to impede Big Brother or Big Zuckerberg or any of the myriad organizations fixated on amassing our personal data.

Second, a VPN is a great way to get access to all sorts of amazing shows and movies and websites that might otherwise be blocked…without spending any extra cash. (This is how I happen to log into one my favorite streaming services, which I won't name for fear they read this and flag my account!)

Third, as a digital nomad living and working overseas, I regularly rely on a VPN to access certain financial accounts back in the U.S. because their networks automatically block my Czech-based laptop from logging in.

Now, I know what you're probably thinking: A virtual private network—it sounds like something that's going to be impossible to set up or use.

The kind of technical jiggery-pokery that's certain to make your blood boil as soon as you try to install it. And sure enough, when I started using them, that's exactly what they were like.

When I got my first personal VPN about a dozen or more years ago, it was frankly a nightmare to use. It tended to work on a schedule of its own choosing or slow my internet speeds to a crawl.

Sometimes it even froze my laptop, which explains my ill-advised, infrequent use of it on my travels.

Today, however, these services have evolved considerably. The industry leaders are pretty much all reasonably priced, reliable, easy to use, and effective.

Here's how they work: A VPN basically creates a secure tunnel to a special server located somewhere on the internet. So, when you connect to a website through a VPN, you first send the data to your VPN server, which then encrypts all the data and connects to the website on your behalf.

Similarly, the data that comes back from the internet passes through the VPN's server before reaching your computer. So, there is no direct link between your phone or laptop and the internet. This is why it's typically safe to use public WiFi with a VPN. Because the data is first encrypted by the VPN, it would be unintelligible to any hacker snooping on the open WiFi.

Expand your streaming options

Now, here's the really fun thing about VPNs—you can choose the country where the server you connect to is located. Then, because you are connecting through the VPN, the website or streaming service will think you are connecting from that country.

Here's an example of how you might use this. Imagine you're in the middle of season one of *Twin Peaks* on Netflix when you pop over to London on a business trip.

Once you get to the hotel, you grab your iPad to continue watching Dale and Harry's surreal investigation into the murder of beauty queen Laura, only to find that the show has mysteriously disappeared from your Netflix options.

The problem is that *Twin Peaks* is not available on Netflix in the U.K. This is known as geo-blocking. Companies, most commonly streaming platforms, limit your choices based on where you are connecting from. You can get around this, however, by simply opening your VPN, choosing a server in the U.S., and hey presto, you're back on the U.S. version of Netflix.

The joy of this is, with a good VPN provider, you can connect to a server in pretty much any country. Fan of Asian cinema? Why not check out what's on offer on Netflix in Japan or Korea? Like British TV? You could try the BBC iPlayer, a free U.K. streaming platform.

Although it's typically blocked overseas, you can access it with a VPN by connecting through a U.K. server. So, you could watch the best of British TV, like *Line of Duty* or T*he Night Manager*, for free.

Likewise, you might find that some U.S. websites won't grant access to you when you're in the European Union, since they haven't implemented the EU's strict General Data Protection Regulations. The image in the next column, for instance, shows what happens when you try to connect to The Baltimore Sun website from the EU. Again, you can circumnavigate these restrictions by connecting through a VPN server in the U.S.

Escape the gaze of Big Brother

A good VPN will not only seriously improve your entertainment options, it can also restore some of your privacy.

Personal privacy, as we once knew it, is on the verge of extinction. Major global governments are seemingly intent on creating massive digital surveillance states or controlling what their citizens do online, as evidenced by the NSA's bulk data collection program, the U.K.'s Snooper Charter, and China's Great Firewall. Then there's private industry. The collecting and selling of our personal data is now the biggest business on the planet.

As *The Economist* reported last year, about $1.4 trillion of the combined $1.9 trillion market value of Alphabet (Google's parent company) and Facebook comes from our data and the firms' mining of it (once you strip out the value of their assets, cash, and R&D).

Even your internet service provider (ISP) is monitoring what you do online and, thanks to Congress, it can sell anonymized data about you.

If any of this bothers you (and it should), a VPN—with its data encryption capabilities—can provide some level of anonymity. It can't stop all the ways these firms track you, such as cookies on your browser, but it can shut down a lot of them. A few pro tips here if you're looking to circumvent government data collection programs.

First, set up your standard VPN connection to a server outside the Fourteen Eyes Alliance—an international intelligence sharing network spanning the world's major Western powers, including the U.S., the U.K., and Germany.

You can assume that if any of these 14 gets access to your data online, your data can then be shared with the other countries. So choose to access the internet through a VPN in, say, Switzerland.

Second, if you're planning to visit China, get a VPN before you go. You can't download one once you're in China. It's also technically illegal for individuals to use VPNs in China, though it has been estimated that as many as 30% of China's web users have one, and there are no reports of foreign nationals being charged for using them.

Which VPN should I get?

There are numerous solid choices for VPNs. The best option for you will depend on what you want to use your VPN for and how much you are willing to spend. Here's my top picks.

Best for streaming: ExpressVPN

ExpressVPN is the VPN I've used for the last three or four years on my phone, my laptop, and my TV. I say that not for any personal benefit from the company. I share it because I know the service works well, and I've used it all over the world in my travels.

The company provides lightning-fast VPN connections, which is great if you're going to be regularly streaming shows in high-definition or 4K. It also offers connections through 160 locations around the world. ExpressVPN offers a 30-day free trial, but it's not the cheapest option on the market. The majority of VPNs are constantly running promotions, so prices can vary from week to week. At time of writing, an annual ExpressVPN subscription was $99.95.

Best for privacy: NordVPN

The biggest name in the industry, Panama-based NordVPN has an independently audited no-log policy, meaning you can be sure they won't keep any record of what you're doing online. Plus, it has more server locations than ExpressVPN. At time of writing, NordVPN was running a promotion, offering a discounted one-year plan for $59.

Best bargain: Surfshark

A relatively new entrant on the market, Surfshark has servers in 65 countries. It's simple to use and unbeatable on price, offering a two-year plan at time of writing for just $59.76. Another advantage of Surfshark is that it offers unlimited devices, meaning you can use the service on as many laptops, desktops, phones, and tablets as you like. (ExpressVPN has a limit of five devices, NordVPN of six.)

My colleague Ciaran started using Surfshark last November and reports zero problems with connectivity. Given its remarkable price point, this is the best option for most ordinary internet users.

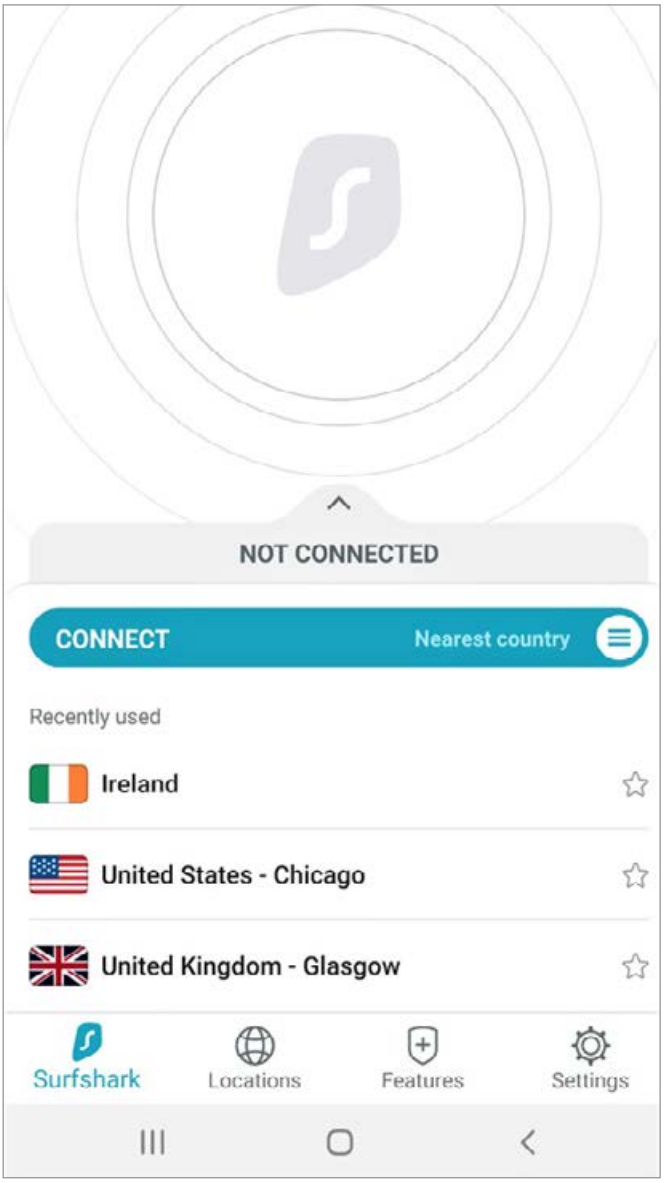
A final thought here is that if you start Googling VPNs, you may come across some free options. Don't use them. Ever. Running a VPN service is expensive. And just like with Google and Facebook, if the service is free, you are the product. Maybe the free VPN is sticking ads in your browser. Or maybe it's selling your internet browsing history to the highest bidder so they can serve you targeted ads. Either way, it's not worth the risk.

How exactly do you use a VPN?

OK, so once you've handed over your cash, now what? Well, it honestly couldn't be easier. When you purchase the service, you'll create your log-in details. Then you'll be prompted to download the software onto your laptop and log in. For phones/tablets, you get the company's app in the App Store or Google Play Store.

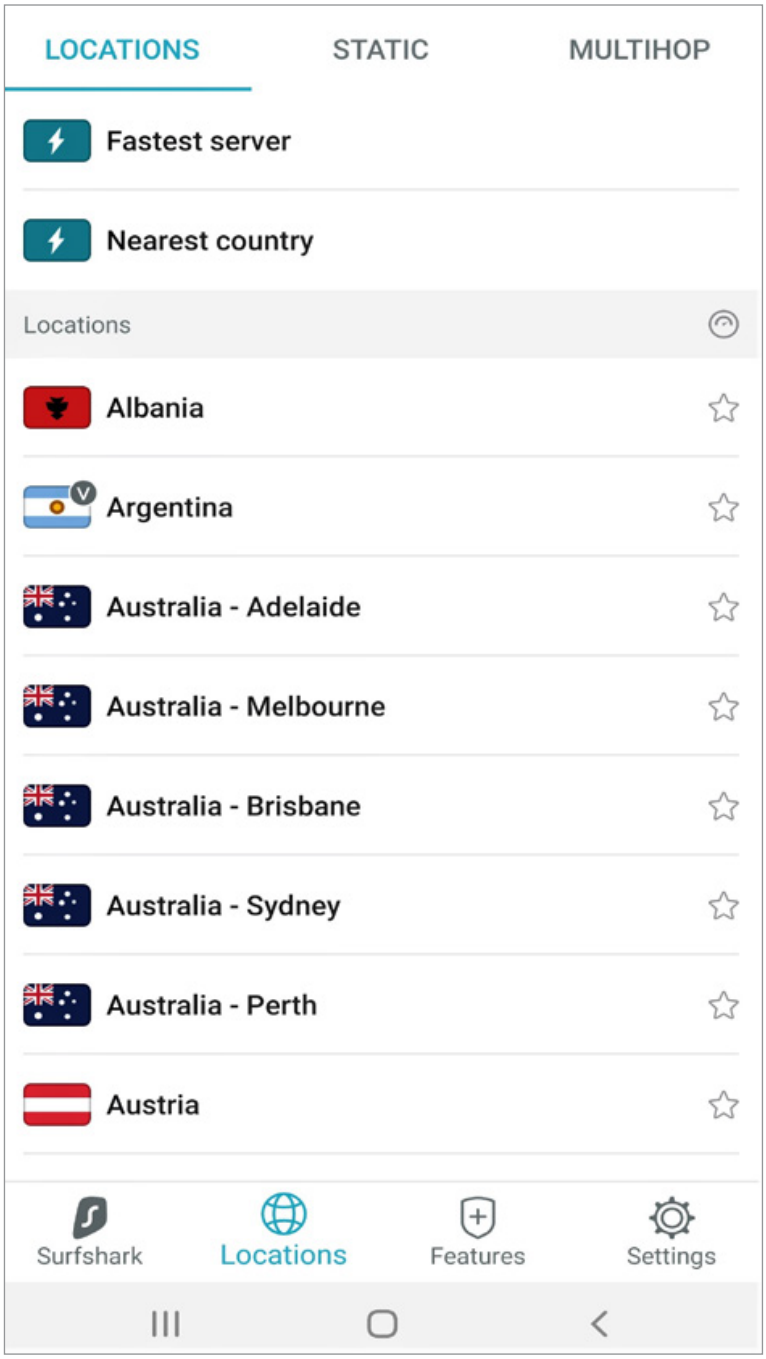
When making a VPN connection for the first time on your mobile device, the software will need to add VPN configurations. Click "Allow" in the pop-up box on iPhone and "OK" on Android. Using these apps is simple.

Let's use the example of Surfshark. This is what the interface looks like:



Once you open the app and log in, you'll see the home screen (above), which tells you whether you are currently connected or not.

Generally, you'll just want to connect to the fastest server in your home country or in the nearest country. You can do this by simply clicking on the turquoise connect button. If you want to change your location to a specific country, you click the location button at the bottom of the screen, which brings up the country list:



As you can see, there are generally multiple servers in popular locations such as the U.S. or Australia. So, you'll always have plenty of options to choose from. That's it. Once you're connected, you'll see the VPN icon (on iPhone) in the top left-hand corner of your phone so you know it's turned on. It's that simple.

As a final note, VPNs do have some practical drawbacks. While VPNs are legal (they're recommended by the FBI after all), some sites look at VPN traffic as suspicious.

So, for instance, it's possible, though unlikely, you may have to turn it off when logging into your bank. The bottom line, however, is that the underlying infrastructure of the internet has not been significantly improved in some time, even though most of us now have multiple devices that are vastly more powerful than the best computers 10 or 20 years ago.

That fact, combined with the reality that we're living more and more of our financial lives online, means it's prudent to err on the side of caution and take every step possible to protect our digital security. Now, to watch the latest season of *Line of Duty* on the BBC iPlayer…

AUTHOR BIOS

Mark Nestmann

Mark Nestmann is the founder of The Nestmann Group, a U.S.-centric consultancy that helps mostly American clients protect their assets, preserve their wealth, and safeguard their future.

His work has been featured in well-known media outlets including *The Washington Post*, ABC News, *The New York Times*, Bloomberg News, *Business Week*, and *Forbes*.

He holds a Masters of Law (LL.M) in international tax law from the University of Vienna.

For more see: *https://www.nestmann.com/*.

Jeff D. Opdyke

Jeff Opdyke was born and raised in South Louisiana in 1966 and has been traveling the world ever since.

He spent 17 years covering personal finance and investing for *The Wall Street Journal* in Dallas, Seattle, and New York, and for seven years wrote the *WSJ*'s nationally syndicated *Love & Money* column that chronicled the real ways personal finances and personal relationships clash.

As executive editor for *The Sovereign Investor* and *Total Wealth Insider*, Jeff traveled the world meeting with politicians, economists, institutional investors, taxi drivers, waitresses, hotel bellhops, and supermarket checkout clerks to better understand local economies and local consumers in a quest to find investment opportunities outside America. His book, *Replay: Your Second Chance to Invest in the American Dream*, was a direct result of those years of global encounters.

Jeff has traveled to nearly 70 countries and currently works as a digital nomad living and writing from Prague, Czech Republic, where he serves as editor and columnist for the monthly *Global Intelligence Letter*, and *Field Notes* daily e-letter, writing about retirement lifestyle, travel, and global investing. He also regularly contributes to *International Living* magazine.