Tangential Vision™

illustration - design - storytelling

conservative values messaging

Handbook

# of Online Privacy

a guide to digital identity integrity

TANGENTIAL VISION'S HANDBOOK

OF ONLINE PRIVACY

a guide to digital identity integrity

Tangential Vision™

illustration - design - storytelling

conservative values messaging

www.tangentialvision.com

Tangential Vision's Handbook to Online Privacy

a guide to digital identity integrity

by

J. James and Mary M.

What has the Biden administration done with their time so far in their first six months?

We are living in the Leftists' long awaited authoritarian moment in history. In July 2021, the White House announced that they have been dictating who should and should not be banned from social media platforms. Your government has been keeping lists of who they think are the spreaders of "misinformation." They are pressuring the corporations they regulate to obey their mandates. This is outright pernicious abuse upon the populace.

After the election of 2016, Leftist propagandists utilized the boogieman of Russian "disinformation" to increase their power to restrict humans to communicate freely. As the following years went on, "disinformation" was switched to "misinformation." What a difference one little letter makes. "Misinformation" we have been told, must be eliminated because otherwise "people will die." Misinformation is information which does not fit the authoritarian narrative, as opposed to disinformation which was (supposedly prolific) overtly-malicious foreign interference in our elections and national narrative.

As of July 2021, the DNC has requested phone companies begin policing text messages for “vaccine misinformation.” Leftist political biases are now enforced in an authoritarian fashion within the public sphere. This vision of cancelling wrong-think on a personal, one-to-one vector should be horrifying to everyone, left, right and center. The historically-educated person will see that this effort won't stop with "vaccines." They will inevitably follow this step by banning interpersonal sharing of election fraud information, genuinely patriotic tendencies, and all manner of anti-governmental sentiment. Indeed, this same month the New York Times deemed the word “freedom” an “anti-government slogan.” A heightened level of oppression has already arrived.

Look at this in context of the march of the Authoritarian-Left. It took just 8 years to go from the Obama administration denying that they spy on our cell phone data to the Biden administration nonchalantly saying they'll fact-check our text messages.

Everyone can see the framing of the “domestic terrorism” issue is being promoted by public television and radio stations in addition to the usual mainstream media corporations. As Glenn Greenwald wrote in a January 19, 2021 article called The New Domestic War on Terror Is Coming: “The more honest proponents of this new domestic War on Terror are explicitly admitting that they want to model it on the first one. A New York Times reporter noted on Monday [1/18] that a “former intelligence official on PBS NewsHour” said “that the US should think about a ‘9/11 Commission’ for domestic extremism and consider applying some of the lessons from the fight against al-Qaeda here at home.”

Every anti-authoritarian in America must now take active steps to erase their digital footprint. There is no reason to believe that someone is actively searching for you, certainly not at this point in the year 2021. This is not a guide devoted to disappearing. The goal of this text is to help people learn how to remove themselves from the data-sharing aspects of the digital world.

In this guide we will cover:

What is a VPN?

VPN stands for Virtual Private Network. A VPN is a simple software that was created to protect your online privacy and make life harder for hackers by anonymizing your traffic and location.

A VPN can help to protect you in a few key ways. VPNs encrypt all the data you send over the internet. When you're connected to a VPN server, all your internet traffic is encrypted. This means that nobody can see what you're doing online, not even your internet service provider (ISP).

The massive shift to remote employment during the pandemic has created a many new targets for hackers. This is because many employees who work from home use insecure personal smartphones and computers, and they don't use encryption. Encryption stops hackers from seeing sensitive information that you enter into websites, such as your passwords or payment information. A VPN makes sure that even if someone stole your data, they wouldn't be able to decrypt it or even understand it.

Your VPN also masks your IP address. The IP address is your computer's unique identifier when you are online. Websites and services, like Netflix, use your IP to determine your location. When you connect to a VPN server, the websites you access only see the VPN's IP address.

Because they can no longer see your real IP, they can't see where you're located. This is essential if you want to bypass geoblocks and censorship. It means you can access any show, movie, or game in the world, and browse with complete freedom in every country you visit.

Some VPNs block malicious websites, ads, and trackers. Malicious websites can download malware and trackers onto your device without you knowing. VPNs with built-in protection help to prevent infections by blocking these sites before they can do damage.

Some also block ads and pop-ups. This stops malicious ads from infecting your device with malware, and it means you can use your phone or computer with significantly reduced risks of infection.

Imagine a VPN as a tunnel your data flows through. Your VPN directs all of your internet traffic through to one of its servers, where it's encrypted. The VPN might send your traffic from America to (for instance) Germany, completely encrypted. From there, your VPN server forwards your traffic to the website you're visiting, for example a website, app, or streaming service. The site sees the VPN server as the origin of your traffic, instead of your device. This means that it also sees your VPN server's IP address instead of yours.

The best VPNs use thousands of servers and update their IP addresses regularly, so sites don't have enough time to blacklist and block them. And that means, you stay completely private and undetectable. There are many VPNs available. Our personal recommendation is Express VPN.

You can also look into getting a VPN Router, which takes an extra step of having the VPN for your system operating outside of your home computer. This means the VPN is already operating and connected before the machine, tablet, or phone you are using is even turned on. This also keeps your home internet, location, and wifi safe when you have guests using it.

How can you safely use email to communicate?

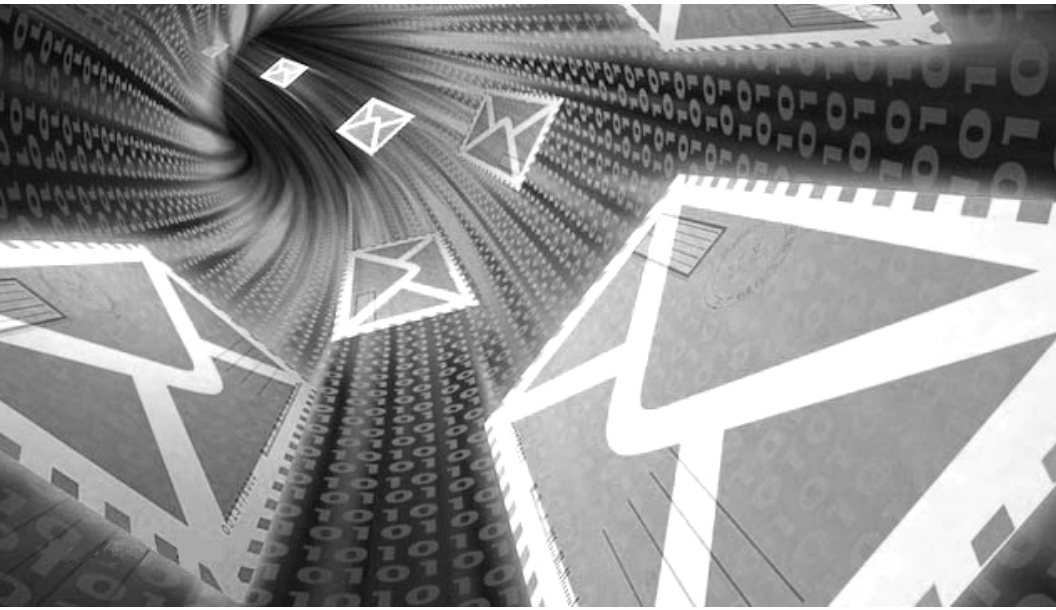
There are many risks involved with using common unencrypted email. Unencrypted email can be accessed by ISPs, hackers, or even anyone in the structure of the email service provider. It should be understood that any common email which is sent will be read and logged by the government, no matter who the sender is or what the contents of the email are. Any number of strangers can have access to the information which is contained in your mail.

Email encryption protects confidential information such as your credit card number, banking account number, and maybe your social security number. Emails also include your personal ISP information and location information, and even “domestic terror” concerns such as your basic political views. Can you imagine your messages being not only read but even altered in transit because you have the wrong beliefs about taxes or authoritarian government?

Hackers will be subtle and try to keep you unaware that they have accessed your email. A friend might get an authentic message first, and then later receive fake messages which appear to be official later on. Worse, if any person gets into your email bubble they will be able to target you for identity theft. This is becoming a more common story. You can avoid this if you use an appropriate email encryption.

Encryption renders the content of your emails unreadable as they travel from origin to destination, so even if someone intercepts your messages, they can’t interpret the content.

Most of us use Gmail. To some degree it is unavoidable since so many services currently require a Gmail account. To safely use Gmail, we recommend only accessing it in a separate browser from every other search or website you access. This will limit the amount of data Google is able to eke out from your computer via the browser.



We recommend switching to Protonmail for your email choice. Protonmail allows you to exercise some anonymity online. Unfortunately the encryption of Protonmail is only end-to-end if the other recipient is also using the same Protonmail service. Nonetheless, this is still a step up from the current email most people are using. Additionally, the number of Americans using Protonmail is currently swelling. Email in general is not a very secure form of communication so it is advisable to keep important personal communication in other formats.

We're also hearing great things about Startmail.

What is a text-messaging proxy?

You might use an online proxy for receiving SMS text services. You might want to register a proxy phone number with an online service to avoid continual advertising to your phone, or to avoid specifically connecting your identity to a minor service. One service we recommend for this purpose is receive-smss.com although there are many sites like this. Use Duckduckgo to search for the keywords “free online text receiving for service registration” and see what options are available. It is very important to remember to save a record of which service and proxy number you used in case you need to return to it at a later date.

While we’re on the topic, don’t use Google as a search engine, silly. Duckduckgo is currently the gold standard.

What is wrong with my cell phone?

Your cell phone is a highly sophisticated data collection and tracking device. Your cell phone sucks.

One easy alternative you can look at is the Clearphone. A private company called Clear has been building decentralized communication options including its own network. They produce cell phones which operate on their own OS (operating system) and these phones use a whole suite of apps created by the same company. They have chosen to replace all of the normal apps which cause security concerns by just making them all themselves.

If you want an easy solution to De-Googling, then Clear might be the answer. This company offers filters and the ability to choose what can be searched and downloaded

onto the phone. Parents can be assured that it offers protection for kid's phone. A Clear phone will uses Duckduckgo as a default search engine. There is still some level of Google software on it.

We recommend taking the effort to purchase a Braxphone. Braxphones are De-Googled, Linux-based, utilize open-source apps only, and third-party app stores. This phone will come with no Google services installed whatsoever. It will prompt the user with a warning when trying to install an app which communicates with Google. It will generally warn the user about apps with invasive privacy permissions.

"De-Googled" – To have a phone "De-Googled" removes all programs and apps which utilize code and software which can be harmful. Many apps communicate with Google, or share your data with other Big Tech corporations. Any popular or useful common phone application has alternative apps available for use.

A properly De-Googled phone operates on an alternative OS (operating system) such as a Linux-based OS. Linux-based OS technology may be the future of online safety. It may be time for conservative communities to begin networking about the advances in their group efforts to institute these sorts of operating systems.

Braxphones are built by a privacy advocate named Rob Braxman. He has a popular channel on YouTube and you can purchase phones at reasonable prices on his website. Be prepared to check it daily for inventory updates, as his phones tend to sell out the same day he lists them online.

It is impossible to completely avoid GPS Triangulation and Tracking. However, there is no reason to believe that anyone is actively searching for you anyway. The focus of this text is to help people learn how to remove themselves from the data-sharing aspects of the digital world to preserve your digital integrity.

Paying online with Privacy.com

There is a way to protect your identity from service providers and product suppliers. This is called Privacy.com. You can use Privacy for online purchases or over the phone. It is not made for using in-person. Privacy is linked to your checking account. Any purchase you make using privacy will show up in your checking account using the payee's actual information, so Privacy only works in one direction: safeguarding you from the data collection efforts of the payee. Your bank will still know about your proclivities.

Privacy protects your real credit or debit card number by replacing it with a proxy number. In addition, you can replace your name with a proxy name. In the case that a service provider is ever forced to provide user data to an authoritarian force, your real data will not be present.
For every use of Privacy you must create a new "card" on their website. So, if you use a certain Privacy card for Lyft, you won't be able to use the same Privacy card for Southwest Airlines. Consider pairing this with a free online SMS text receiving site like receive-smss.com.

Tell me more about apps

Apps talk to one another. They collect and share your data. This is called data mining. Most people think that apps are

fun and free, but if you are reading this you probably already know that apps are not free. You pay for them with your data and privacy. Even gaming apps are not created with the purpose to entertain, they are meant to make money using your personal data. *You are the product.* Consider ditching the Google Play Store and use Aurora Store and F-Droid instead.

Here are some replacement apps worthy of your consideration. Instead of YouTube, use NewPipe which acts as a YouTube proxy, it doesn't track your preferences. This will stop Google from tracking your watch history. Instead of Google Maps you can use Waze for GPS services. You can replace your default SMS text app with Messages. There are alternatives for every app you would commonly use, and so just do your research as you remove and replace your commonly-used apps.

Always try to use open source apps. Also please take the time to investigate each app to see which permissions it requests or requires. Many apps say that they "require" Google Play Services but will function without it. It is important to understand that the Play Store wields a powerful near-monopoly on distribution of apps. Some apps are even designed to function poorly without regular updates from Google, however there is an app called FakeStore which will fix this issue. The FakeStore is a stub that disguises itself as the Play Store: FakeStore shares the same package name as the Play Store com.android.vending. This prevents some apps from crashing. This is not a problem which we have ever encountered yet, although one day it may happen and so we are prepared in advance.

Safer texting using encrypted apps

There are many encrypted texting apps to supplement or replace your normal SMS texting apps. These are three which we recommend looking into, from least to best.

Signal –

Signal is best when used between family or commonly known contacts. If both parties have Signal installed, it will allow voice calling or video calls in addition to texting. Large groups can easily share information, links, or opinions in real-time.

Signal requires your phone number and displays it to anyone you communicate with. This allows for social contact tracing and can be a liability in large groups with unknown participants.

Social contacts can be used to trace you and identify you. Sometimes it's more important to protect "who" you're talking to, even more than "what" you're talking about. There are also persistent rumors that Signal was created using government funding and three-letter intelligence

group guidance and oversight similarly to how Facebook and Twitter were created.

Signal has a great feature of automatically notifying you if a new contact in your phone is also on Signal. It does have great value for large groups info sharing, family communications, and quick one-to-one chat.

Wire –

Wire is a well-regarded collaboration suite with secure messaging, group chat capabilities, file-sharing, and the ability to collaborate securely with external clients. Wire has the benefit of being 100% open source code. The code is available on GitHub. It has shifted from a personal focus to more of a corporate-client user base but is still available for all.

Wire's code has been independently audited by third parties. The option to register using a (potentially throw-away) email address offers more privacy than those services that force you to enter a phone number when a new create account is created.

Personal users can know that strong privacy laws were kept in mind by the creators of Wire in addition to strong encryption. All user data is stored locally, in encrypted form, on your own device. Storing all user data in an encrypted form on user devices is a strong security move.

As with like the previous security-texting app Signal and the following app Session, Wire does allow for self-destructing messages.

Session –

Session is an end-to-end encrypted texting app which minimizes sensitive metadata. The identity of the Session users are completely anonymous. Session is designed for absolute privacy and freedom from surveillance.

Session can be somewhat complicated to install for less tech-savvy users, however it only takes a few steps. Combined with a text-messaging proxy for setup, Session can give the users complete anonymity. It does not require email or continual connection to a phone number which can be used to find out your identity.

Session cannot be directly accessed by the user's ISP. It is not connected to contacts, so it cannot be used for contact tracing. This app also supports group chats for information sharing.

This app can be used on either a cell phone, tablet, or computer. It also allows multi-device synchronization so you can receive texts on your work computer at home and also on your cell phone while you're out.

Users can copy and paste their unique 65-digit user ID to each other to connect, or send a qr code as an option instead. This makes connecting more easy and secure.

Session does need a strong internet connection to function. It can work while on the move but generally needs a wifi signal to operate. This can include public wifis such as at the store, or sitting outside a restaurant. Session is the strongest encrypted texting app but also the most difficult to use and hardest to get friends and family on to.

Why and how to avoid contact tracing

Contact tracing is now becoming normalized. Before 2020 any person who talked about contact tracing would have been considered a crank. Now in 2021 any person who thinks that contact tracing isn't great must somehow be evil. How quickly the public opinion can switch gears.

Your phone shares your contacts. If by chance one of your friends has managed somehow to keep their phone identity completely anonymous then when you save their name in your phone their identity will be verified by you.

Moreover, the gps of cell phones is now being used to identify on a real-time basis who you have met in public and the exact path of your steps over time. A friend recently told me that his Google Maps path of movement record went back at least nine years.

Everything is logged and recorded: emails, calls, texts. Your cell phone will now be used to not only track your movement, but also to track who you come into contact with. This should be of great concern to anyone who realizes that the government has already publicly

announced the full intention to use the military to go after private citizens based on their political views using the same methods and degree of force they have with Al-Qaeda and Isis. Could we see the homes of Proud Boys and Antifa receiving missile attacks in the near future?

This technology will not simply disappear once the pandemic is over, if they ever allow the pandemic to end. Governments and law enforcement will now be able to easily squash not only open dissent but even passive opinions which do not fit the narrative. No longer does someone need to consciously inform on their contacts. Their phone will have already done that.

You might not have anything to hide; most of us don't. However, as we can see now with COVID-19 and have seen with patriotic Americans in the past year, you don't need to commit a crime for them to come knocking on your door. You just need to have been near someone.

Use encryption to avoid large digital rolodexes of contacts. Signal can save phone numbers separate from your phone's directory. Notepad documents can record some numbers as well. Consider different ways to keep track of friends which don't rely on digital methods.

Using web browsers as a tool instead of a liability

One powerful technique you can use to protect your data from Big Tech is "browser segregation." Browser segregation is the practice of using a variety of different web browsers to separate your online data. This may include purchases, searches, and services used from the more aggressively malicious services and data miners.

The biggest concerns in this matter are Google, Facebook / Instagram, Amazon, and Microsoft. Runners up include AOL and Yahoo. These are the world's the world's biggest data aggregators.

These aggregators can (to various degrees individually) not only collect the data you volunteer to them intentionally but also collect data from other open tabs in the browser they are being used in. Facebook is probably the most aggressive in this sense, Firefox even developed a "Facebook Fence" plugin years ago to try and contain Facebook's snooping.

The easiest way to fix this problem is to completely stop using these services. This is not possible for many people overnight, however. The next best thing is to utilize a variety of web browsers to keep each of these isolated from one another and from your normal web usage. To do this we recommend a minimum of 3 separate browsers. During a long enough work period we might have up to half a dozen browsers running at once.

Technically it does not matter which browsers you use as long as they start out cleared of history and cookies, or with a completely fresh installation. We suggest using Chrome for anything which requires Google products to be accessed. This way Google only knows the Google-related business. You could then use Edge for Facebook / Instagram and keep Facebook from accessing everything you do in their aggregating. YouTube falls under the Google umbrella but I like to use a separate browser for it as well. We suggest a different browser for Amazon as well! One of us uses Brave for personal web browsing, the other uses Firefox. There are so many browsers available.

Firefox used to be considered a secure browser, however it has fallen out of favor with privacy advocates. So-called "onion browsers" offer the highest level of decentralized web access. These include Tor and Brave. They are called onion browsers because they operate using a node-based form of communication, meaning it has layers of secure connections. Dissenter is a great new option for this as well. We recommend Dissenter for politically-oriented browsing or writing.

If you are using the more private and secured browsers, you might have a difficult time signing in to certain accounts or accessing some web pages. We have found that by using a VPN and practicing browser segregation, our protection from data-mining companies is already significantly better than by not having a plan.

GENDER NEUTRAL NON-BINARY OLDER SIBLING

IS WATCHING

You have a need for a professional illustrator and designer. A conservative who knows how Marxists think. Let me share my vision with you. Here are the ways we can help each other and how ***I can be of service*** to your cause and the broader patriotic movement.

1. Option 1: Creating directly for your group's "personal focus" event or small local cause. Making something which is a "one-time" project.

You have a vision! You need to see it completed in time for your event. Tangential Vision will create the perfect messaging for your group to share your cause with your local commmunity .

costs: estimated on total individual project time, scope of use, and scale of organization

2. Option 2: You need something which can be beneficial to other nearby conservative groups in the same or neighboring counties.

Your group has a concept or idea which you believe will change the hearts and minds of the community, and the concept might be able to be extended to other nearby areas.

costs: similar to Option 1 but reduced costs because TV would be able to reuse the imagery

3. Option 3: Taking part in Tangential Vision's larger goal creating a "broad focus" network of conservative messaging across the county lines.

Your group wants to be able to influence the hearts and minds of the local community, tap into the rising spirit of resistance, with pre-existing roadside signs, lawn signs, and flyers.

costs: a small licensing fee for the reproduction of conservative messaging, based on scale of org.

4. Option 4: Purchase Tangential Vision's products such as informative brochures, booklets, shirts, and stickers to share the "broad focus."

Your group wants to invest in some inventory of products to hand out at events and resell at fundraisers. You as an individual see some great conservative messaging you want to show off!

costs: per item or package based on your own budget and desires

5. Option 5: Donate money to support the cause. 70% of donations will go toward production runs, product design, and growing the business.

Tangential Vision is a time consuming one-man concept and needs the support of the conservative community to work. You can donate any amount directly to major goals such as large-scale messaging within my local community and you would be supporting this cause.

costs: Tangential Vision is happy to accept any general seed money to support the "broad focus"

www.tangentialvision.com

If you would like to embark on a deeper dive, we would recommend researching these other companies: Acxiom, Accenture, LexisNexis, Response Unlimited, ChoicePoint.

Conclusion

We live in an Authoritarian Leftist moment in history. The government is openly practicing censorship and abject political persecution. Social media platforms are being used to groom lists of noncompliant citizens. Corporations are blended fully in with the government structure, financial bodies, united in abject hatred of this nation. The level of outright pernicious abuse is only beginning and we can expect it to increase in momentum.

So-called misinformation will continue to be used to identify anti-authoritarians and create a moral causation for isolating and attacking them. The authoritarian DNC is paired up with basic service providers to enforce their dystopian vision on a personal, one-to-one basis. This is Fascism in every sense of the word.

The common man is either in the conservative camp which believes that freedom belongs to everyone alive, or been bullied into Leftism beliefs that nobody should be free and that slavery is freedom. The definition of “terrorism” will continue to be broadened by public television, radio stations, and mainstream media corporations.

Every anti-authoritarian in America should be taking active steps to erase their digital footprint. Past is the time when this act was not a most vital concern for every man, woman and child. Everyone alive can feel that NOW is the time for utmost urgency. Safeguard your life.

It took just 8 years to go from the Obama administration denying that they spy on our cell phone data to the Biden administration nonchalantly saying they'll fact-check our text messages.

But hey, Trump was the Nazi, right?