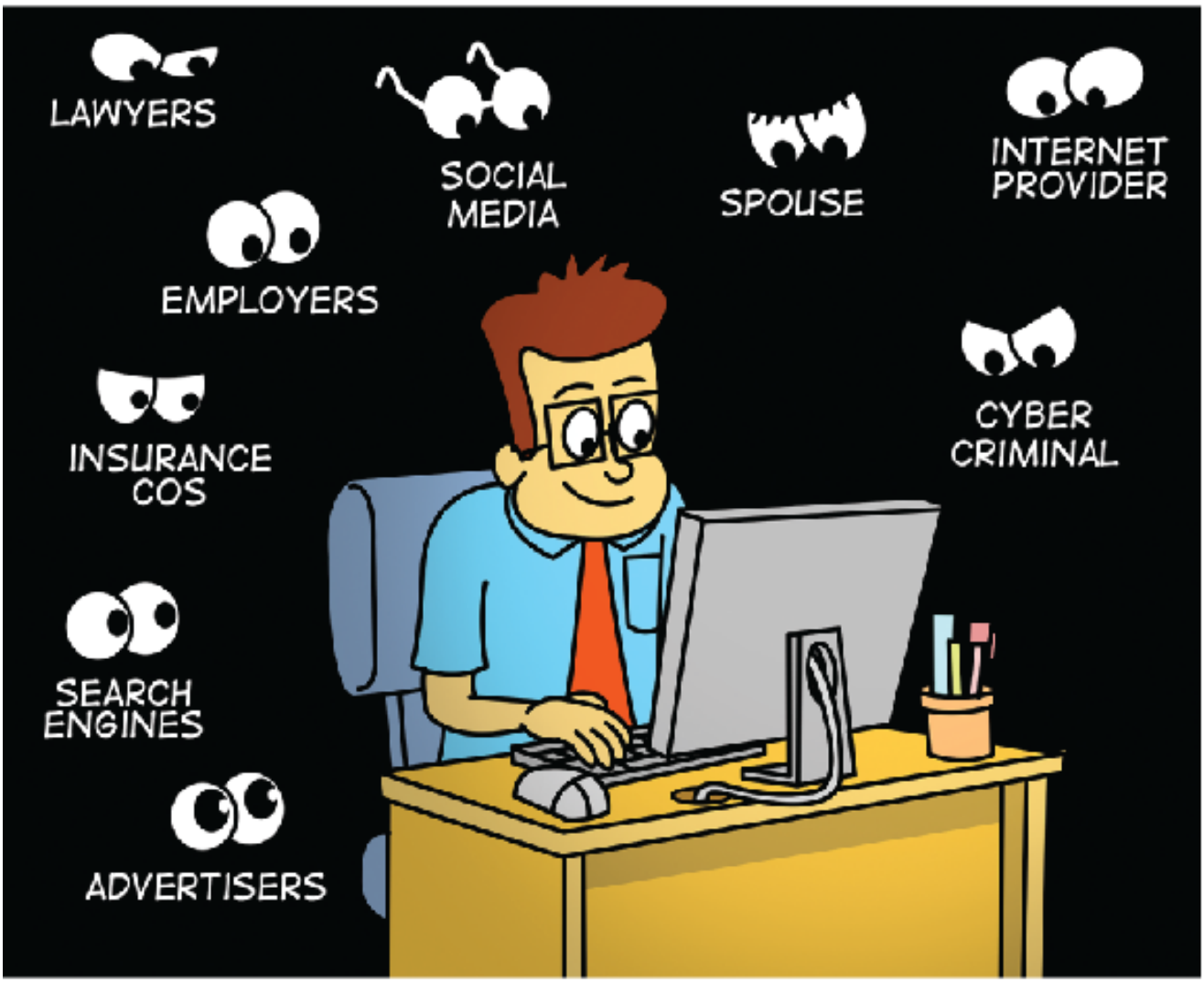
ONLINE PRIVACY SECRETS REVEALED

DON'T LET YOUR BROWSING BE USED AGAINST YOU



THE FOUNDER OF TRACEFREE DISCUSSES THE MYTHS OF PRIVATE BROWSING, AND SHOWS HOW YOU CAN FINALLY BE SECURE AND ANONYMOUS ONLINE

(Bonus included: 10 Ways to tell if you really are private and secure online)

"On the Internet, nobody knows you're a dog."

(source)

The year was 1993, and you started getting those AOL CD's in the mail. It would still be a couple years before Amazon would open their virtual doors, and 5 years before you would start giving your personal data to behemoth Google. Peter Steiner, a cartoonist and contributor to *The New Yorker*, posted this cartoon which marked a notable moment in the history of the Internet. Back then, you **could be** a dog, or certainly anonymous on the Web.

Fast forward 25 years later and Big Tech can now tell what kind of dog you are, where your kennel is, favorite food and toys, along with your internet playmates and where you "mark your territory".

Through years of Web browsing on different devices, Big Tech has created a very detailed online profile on you. The disturbing thing about this is, **for right now**, it's only being used to deliver targeted online advertising.

Intro

For the past 10 years, experts and media have been telling everyone to use the "private" mode on their browser to surf privately. Because of this, people have been misled into thinking they were browsing privately. In fact, in the vast majority of cases they were actually sharing their most private browsing with the world's largest information gatherer, namely Google.

This year (May 2018) the EU's General Data Privacy Regulation (GDPR) and the Cambridge Analytica/Facebook scandal shone a light on just how much information the Tech Giants are really getting. More importantly, SHARING this information without your consent, proving how little privacy you really do have online.

It was at this time, these same "experts" discovered that surfing in "private" mode isn't really private at all.

To make matters even worse, after all the stink that was made about your online privacy, a new law that TAKES AWAY online privacy was passed and not many experts are talking about it at all. In April of 2017, law SJR-34 was passed that basically allows Internet Providers to sell and share your data without your consent! Although there has been talk about repealing this legislation, this law is bound to have enormous ramifications on web browsing.

Rather than look for a solution, these so called experts are now recommending another ineffective technology for private browsing.

With this background in mind, the purpose of this book is to give readers some vision as to where the Internet is headed. It's also meant to educate you about the current browsing solutions and how they relate to your privacy and security. We want to make sure you don't make the same mistake again, when believing your security and privacy is protected using the technology and browsing solutions under the current landscape, when in fact it is anything but!

Chapters:

1. Biggest Myths of Private Browsing

Here are probably the 5 biggest myths of private browsing:

1. You can be private online. **FALSE...** Users can never be private, you can ONLY be anonymous.

2. Your browsing is private when using *incognito/private mode*. **FALSE...** ISP's can see your browsing history. Websites know who you are, sites you visited, and can track you online.

3. Your searches are private when using a private search engine. **FALSE...** Between your device, browser, and ISP, there are enough clues for the largest search engine in the world (Google), to tell what you searched for.

4. Your browsing is private when using a VPN (Virtual Private Network). **FALSE...** VPN's do NOT prevent your device from interacting with a website, thereby revealing your identifying information, along with exposing your device to malware and cookies.

5. Encrypted data means it is safe to open. **FALSE...** Just because your data is concealed (inside of a box), does **not** make it safe to open.

We'll show in detail why each of these are very false, and if you are using one, you're not as private or secure as you think.

A lot of words that relate to online privacy and security have been bastardized. Terms like private, incognito, encrypted, and proxy have been thrown around to give users the illusion they are private and/or secure. It took the market 10 years to finally realize that Google's *Incognito*, which was being touted as a private way to browse the Web, isn't really private at all. Heck, Google even told you so on their site, but did anyone bother to actually read it?

We won't confuse you with high tech terms or processes, so we try to "dumb it down" as much as possible. We simply use the expressions "shakes the hand" or "touches" to convey when a user's device connects to a website, to paint this picture**.** Of course the device does not literally touch the other device, BUT it does connect and can transfer data from one device to another. This data can be cookies, documents, videos, viruses or malware.

The next time a newscaster or tech expert starts talking online privacy, you'll be able to tell how educated they are on this subject matter. So at this juncture, let's begin our educational journey.

2. The Information SuperHighway

This is the Internet in a nutshell. Users are either looking for information/entertainment/, an item online (consumer), or they are looking for people to discover their information/entertainment/item online (website).

A software program and an Internet connection allows anyone to find any type of information for FREE. However, there's an old saying if it's **free**, *you are the product,* not the consumer! It's a pretty much accepted fact, that when you don't have to pay to use a service, the information you give while using their service **will be used** by them to generate revenue. Your email is a perfect example of this.

When browsing over a period of time, the more devices used, searches made, and websites visited, usually results in the more personal and relevant your information becomes. This browsing history across **all** devices allows MANY organizations to build a VERY detailed profile of you.

Up until now, your browsing history has only been used to deliver relevant info and targeted ads. A $100B industry has been created by providing relevant information as to **who, what, where** and **when** YOU visited. The importance of this chronicalization cannot be understated, because a whole new industry is being created from your browsing history and it relates to **WHY** you are searching for this info.

Here's an example of the next dimension of browsing. Let's say you search for auto body repair in your zip code. Did you know auto body shops pay advertisers to have their listing show up top? You click on Joe's Body Shop and it's a win win right? You were looking for relevant information, and the search engine provided it. Remember though, Joe paid Google to make sure their site was found. That's basically how it works now.

Google and other Tech Giants have turned the Information SuperHighway into a gigantic universal data aggregation, marketing and profiteering Autobahn/Interstate for their benefit. Yes, Information SuperHighway indeed.

Hopefully readers can see why our aforementioned passage of last year's SJR-34 law, not only enhances Big Tech monetarily, but purposely does NOT address true privacy and security. That's the last thing ISP's, VPN's and companies like Google want! To recap, this new ruling now allows your Internet provider, the company YOU PAY to use the Net with, to sell and share your browsing history **without your consent**... (this also includes those free Wifi hotspots you connect to). That means information about every website visited, search made, and every video you watched can now be sold without your permission. Follow the money and behold the REAL connection here.

Conversely, a revolutionary new technology called TraceFree, allows users to unrestrain themselves from this Big Tech monopoly chain with true privacy and security. We go into great detail explaining this wonderful new TraceFree technology, and all its' benefits at the end of this educational process. Users of TraceFree don't have to worry about all the ineffective privacy policies that have been created.

Speaking of these so called guidelines, **all of those privacy policies that were created, are really useless if the Internet provider can and will share your info**. We'll explain why your Internet provider will be eager to share this later. But first, let's look ahead a bit.

3. What The Future Holds and Ramifications

The future is a "digital background check" that includes your browsing history. We can see any insurance provider, credit card, financial institution, employer, legal, dating site, etc... wanting to do/get a digital background check on their current clients, prospects, or competitors.

Now the answers to the questions (religion, political, sexual preference etc...) that are not legally allowed to be asked on an application or interview, can be answered...

It's no secret, employers look at your social media more than your resume when evaluating a new employee. With that in mind, your social media is what you WANT to show about yourself publicly. Likewise, ANY browsing history is really your private life.

Who else do you think would also pay to have this information? Who could stand to benefit from knowing WHY you were looking for auto body shops? Don't you think your auto insurance provider or your lender/lease company would like to know that your car may have damage? Aha!

Let's get a little more personal. You've heard the medical term pre-existing conditions. Health insurance companies are prohibited from discriminating against people with pre-existing conditions. When you do a search online for a medical issue, couldn't this potentially be considered a "new condition"? Right now, there is NOTHING preventing an insurance company from changing your rates or ending your policy because of this. Wouldn't your health insurance provider be interested in ascertaining this? The answer is quite obvious.

Knowing this, you can change the search to ANY topic and bet there will be PLENTY of parties interested in garnering this information… and with the new SJR-34 law, your Internet provider can sell it to them ***without your consent.***

When sitting down with your lawyer or doctor, you have legal confidentiality. Of course, that entails what you share with them **cannot** be shared without your consent. Asking or sharing information with them is kept confidential. In stark contrast, when asking or sharing information while searching and visiting websites, your confidentiality is definitely NOT guaranteed.

With this reality in mind, is there anything remotely close out there to be truly secure, safe and private while browsing?

4. A Life or Lives?

We recall the story about a young teenage girl that got contained advertisements concerning maternity clothing and nursery furniture coupons for baby items in the mail. Because of this, her father went berserk against the retailer, until he realized his daughter had searched for pregnancy info online. Imagine, getting a coupon in the mail is creepy, but having ads that pertain to searches that follow you online is even creepier! But wait, it gets even more disturbing … and unfortunately, you won't even know it.

Going forward, the database and subsequently advertisers, will know how to advertise to the girl who is pregnant based on her search/online activity. Searches like, "What foods do I need to eat during the first trimester" "planned parenthood clinics near me". This is the kind of information that will be used to target her and every device she uses in the future.

Here is the really creepy part. Because there are honestly only 2 "TV channels" in the U. S. (Google and Facebook) when searching the web, they **have the ability to influence your decision making without you even knowing**. How's that you say? It's is called subliminal advertising, or rather messaging. Consider this reality. Namely, the use by advertisers of images, stories and sounds to influence consumers' responses (or behavior) without their being conscious of it.

Now, in the case of that teenage girl, let's say Facebook pushes pictures of her older sister's baby higher on her news feed. Maybe Facebook will do this? No, there is no maybe about it here. Do you think images/stories of cute babies, deformed babies, or stories about single parenting, could impact her decision on what to do? Furthermore, let's say she is considering an abortion, what if her favorite site highlights a story about a celebrity having one or deciding against one? Or the site highlights new baby pics from a movie star? There are SO many ways a website could influence a decision without her even being aware of it.

This influence can be used for some of life's biggest decisions (divorce, bankruptcy, elections etc...) and Google and Facebook have already been heading down that path!

Ok, so we have pointed out the obvious about decisions being made by users based on their data aggregation while surfing, and all the associated targeted ads tailored to them based off this activity. But there is potentially an even more dark side in play here, where the lines between **legality, good...** and yes even **evil**, can become a nightmare. Legally speaking, a life or lives, could be directly impacted as well based on your internet activity. Consider the following:

Your browsing history gives answers to the questions that are not legally allowed to be asked on an application or in an interview. These include topics such as religion, political and sexual preference etc...

Example; Joe uses a private search engine to find "alcoholics anonymous meetings" in his area. Now, we know he isn't private at all, but let's show you what **could** happen!

That night, he goes to a meeting and naturally brings his cellphone. Innocently enough, and certainly NOT by choice, his cellphone gives him away. Not only that, but now all of the other cellphones in that room can be linked to each other and that AA meeting (not so anonymous anymore). Many participants in these type meetings are looking for emotional support, friends and contacts to share their stories with because they are in the same lifeboat. See the unintended conundrum here for everyone Joe shares his email and contact information with through his phone and their devices?

Alas, what you do on one device gets shared across other devices. Your IP address puts other devices at the "scene of the browsing". Not just the one you're browsing with, but the ones that are using the same "pipe" internet signal IP address… Yes, that includes the one in your pocket.

Unfortunately, here are the potential ramifications between the aforementioned *good, evil* and *legal* in this particular scenario:

Good: The internet provider could send Joe (or his sponsor) a reminder that he hasn't been to a meeting in a few days.

Evil: The ISP can notify his auto insurance, health insurance or employer that Joe is an alcoholic. What do you think happens with his insurance premiums? What about all the OTHERS, along with their phones and devices he shared contact information with?

Legal: Let's say Joe filled out his auto insurance application and checked "casual drinker" or ONE drink a day. Does this information on his application, or perceived lying nullify his coverage?

5. It's About More Than Privacy

2 TV channels

In this chapter, we refer to Facebook and Google as the 2 TV channels, because combined they represent roughly 90% of Internet advertising. Obviously, when 2 companies control that much of internet advertising, it's kind of like the pre-internet old days when there were just 3 TV channels (ABC, CBS and NBC). Following that analogy, there are oodles of TV programs (websites) now, but realistically only 2 TV channels (Google and Facebook….Youtube is owned by Google).

So, let's say there are 2 movie theaters in your town. One is just 2 miles away, but they are known to use subliminal advertising. The other theater is about 15 minutes away and they don't. In this case, they are both showing the same movie. Which theater do you go to? That's right, NOBODY likes to be influenced without their consent!

Where it gets ominous, is how the TV channels can influence your decision on ANY major life decision, without you even knowing about it… and there are NO laws against this!

That was the case in our earlier example of one life, but let's consider how the bias of the 2 TV channels can influence internet surfers (without them even knowing), to change the lives of millions.

Similarly, your local paper or news channel announces they are endorsing candidate X, or legislative bill. Any rational person now knows, that news channel will be undoubtedly be biased in favor of that candidate or legislation.

Just like there are left and right leaning websites, there are right and left leaning news outlets as well. Consider the following questions. So what do you do when the only 2 TV channels have very publicly endorsed one candidate? When the CEO of the largest TV channel funded (and publicly endorsed) one of the candidates and also wore a staff badge? When a founder of the 2nd largest TV channel **also** funds the same candidate? When the COO of the 2nd largest TV channel says "*I want candidate X" to win badly*"? Quite a conundrum of facts and questions indeed, for someone initially purporting to be neutral before this exposure!

Do you honestly think your “news” (and the content that you get on the Internet) will, or can be unbiased when it comes from the **only** 2 TV channels? Remembering here, they know everything about you, and may have a financial interest in influencing your decisions!

In reality, Eli Pariser in *The Filter Bubble* (book link), calls it *“persuasion profiling”.*

“In the wrong hands, persuasion profiling gives companies the ability to circumvent your rational decision making, tap into your psychology, and draw out your compulsions.

Understand someone’s identity, and you’re better equipped to influence what he or she does”

Taking all this into consideration, if I’m the content deliverer and know all of this information, through subliminal messaging (pictures, stories, videos and ads), I can influence the WHY of your browsing right now. More importantly, I can influence some of your biggest decisions in life and you would have no idea I was doing it.

Now folks, that is really beyond creepy.

Above all here, we’re NOT saying don't use Google, because that’s almost impossible. What we ARE saying, is you can NOW use Google without them knowing who you are or having your profile (browsing history) being used against you! In effect, USE Google without them using you. With this intention, using a disposable browser, so there is no past to be used in your future. Employ the only virtual private browser with complete anonymity and security, so you are ALWAYS anonymous and your browsing (past and future) cannot be used against you!

Think of this another way, when visiting stores in the mall, one would certainly NOT give out their name and email if they didn't buy a product. Would you? In fact, most sensible people would AVOID those stores altogether.

So when people say, “why do I need a private browser?” We say private browsing is so much more than just for embarrassing searches, best online pricing or visiting naughty sites. Because of all the aforementioned pitfalls, it’s simply for unbiased surfing. Your past browsing history cannot be used against you. Perhaps even more importantly, it now cannot influence your future web browsing and decision making.

With this reality in mind, is there anything remotely close out there to be truly secure, safe, private AND deliver unbiased browsing?

Well, the answer is a resounding YES. Now there's a new movie theater in your town that offers the same top running movies and doesn't advertise subliminally to you! With that, let's take a look at two of the biggest misnomers in the industry.

6. Private and Anonymous...What's The Difference?

Before we begin concerning this difference, clarification is needed on two words that are being used incorrectly. These are words that people use interchangeably, but they mean two VERY different things.

First, the term private can best be defined as this online… your identity and online activity are completely hidden. Being private online is IMPOSSIBLE, because (in spite of what some products say) you cannot hide your digital footprints. However, you CAN wear someone else's shoes, which effectively hides YOUR digital footprints.

Second, the term anonymous means that your activity IS visible, but your identity is NOT. User's online activity can always be seen, but who's actually behind the activity cannot!

An easy analogy for these two words is found comparing a wooden door versus frosted glass. When you are behind a wooden door, nobody can see who you are or what you're doing, and THAT is being ***private***. On the other hand, with frosted glass your activity can be seen, but your identity isn't. THAT's being ***anonymous.*** We would also like to add here, while using TraceFree, your browsing is always ***anonymous***. Only if you login to a site, do you let them inside the room with the frosted glass. Put another way, Big Tech like Google, Facebook and Amazon et all, can come in that room if you exclusively login to their sites.

There's no such thing as private browsing, only anonymous surfing. Because the industry has falsely described "private" solutions, we will use the term **private** going forward. Important to remember though, TraceFree enables you to hide who you are by wearing someone else's digital shoes.

Almost 10 years ago, Google introduced their private form of browsing, called *Incognito Mode*. Users could simply click a tab on their free Chrome browser and they thought they were browsing privately. A black hat, mask and background appeared to give one the illusion of being private. For many years, tech "experts" were telling their readers, this form of browsing would keep them "confidential/private". So, for 10 years people were thinking they were privately surfing, but all the

while letting Google know everything about them. Well today, those same experts are telling users they are not private whatsoever with Google's *Incognito* (link)

As previously mentioned, this was in spite of the fact that Google told **everyone**, you're not private on their Incognito website.

Those very same "experts" are now recommending, in order to be private and anonymous, online users need to do two things. Either use a VPN with their browser when surfing the Web, OR if they want to hide their search history, use a private search engine! This is the same technology that came out just months after Windows 95 was launched. Yeah that's right, 22 year old technology!

7. The FOUR Points Of Browsing

Maybe you never considered it before, but there are actually 4 points in the "loop" when you browse the Web.

1. **Your device**. Whether it's a PC, laptop, cell phone or TV, this is usually the most valuable part of the cycle, because users typically store A LOT of personal information on it.
2. **The browser**. Chances are your browser came with the device, or you very easily downloaded one, AND it's free to use.
3. **The Internet provider**. You need an Internet connection to surf the Web. Most of the time it's your local provider (home or cellular), or you may even use a WiFi connection (hotel, airport etc...).
4. **The website**. When visiting a website, your device and browser shake hands with the owner of the website (another computer). Every single website on the internet has a unique IP address assigned to it. So when you click a link or type a URL, the browser is really trying to access the IP address belonging to the computer which hosts the server of the website you're requesting access to.

When you use a VPN (Virtual Private Network) with a browser, you're adding another point in this loop. We will discuss this later, but more important at this stage is the following fact:

What users will find, is these "private" browsing solutions may keep them anonymous with a couple of the 4 points, they do **NOT** keep you private and secure on all 4.

8. Key Facts About Encryption and VPNs

Just what is encryption? It is defined as "*to conceal data in (something) by converting it into a code*".

Many browsing solutions (browsers, Virtual Private Networks, even search engines) love to throw this word around and make you think you're private and safe, when in fact you are NOT.

Encryption when browsing, simply means *to protect sensitive **information** transmitted online.* Only the sender and encrypter know what is inside the information, but that DOES NOT mean what's inside is safe! Another key point to remember, it also means the sender and receiver's computing devices interact with each other. You are not private or secure from a website when you browse with a VPN, or a browser that says they encrypt your traffic.

Let's be crystal clear here, **encrypted data does NOT mean the data is virus free.** It simply means the data is "packaged" in such a way, that only the sender and receiver can decipher it.

As an illustration, you may well be hiding what you're doing from Fedex/(Internet provider), but the recipient knows who you are. In this case, they can touch your device and possibly infect it. When using a VPN, you're NOT private or secure as well. The VPN also knows where you surfed too.

Not only that, but when using a VPN, your device shakes the hand of the other computer and opens the package. Think about it for just a moment, do you open packages from unknown senders?

Now, there are providers that say they use military grade encryption, or the highest rated form of encryption. The next time you hear that, just think of it as using the best duct tape on the package. It doesn't make the package with a bomb inside any safer to open.

This is simply the "latest thing" experts are recommending you use to be private online.
In the future, when you hear the word *encrypt* being used to make you feel safe, realize that ONLY YOUR DATA is secure, but your device is not!

9. World Wide Web and Your Passport

Surfing the Web is kind of like traveling the world. With that being said, your passport contains very identifying information about you. When visiting a country, the border agent scans your passport to identify you and see what countries you have visited before. This information is stored in a world database that can be viewed. Of course, this is done primarily for security reasons.

Similarly, when you surf, each time you visit a new site is like using an Internet passport. Your browser and device are "scanned" to determine who you are and where you came from. This info is stored in MANY databases, and is used to deliver a more personal browsing experience, or deliver targeted ads.

Now, some browsing solutions will make users think they are private by altering their browser/"passport" and say you're private. Some solutions will change or hide the cover of your passport. In addition, they will take out all the stamped pages, or put false stamps inside the passport.

However, as soon as the passport is swiped at the border, your true identity and your travel log is revealed. In effect, the same exact thing happens every time you browse when using these solutions.

The ideal way to surf the Web completely private and secure, would be to get a one-time disposable passport from a different country. In effect, this gives you someone else's identification EVERY TIME you surf. Think of it, each website would indeed see a person, but NOT you! They would think you came from country X, but you really came from country Y. Equally important, they could/can never tell where you really went online.

During your visit, the site would think you were someone else. Yes, they would stamp this passport, but it's NOT yours. The travel activity still goes into the database, but it isn't associated with you. Furthermore, when you are done surfing, the passport is destroyed. Now, that would be ideal. The great news is, it's available today!

10. Cut the Cord… Triple Play

Remember when we said earlier, that there would be a big incentive for your Internet provider to sell your browsing history? Let's revisit new law SJR-34's financial impact, that lets your Internet provider sell and share your browsing history without your consent.

Recall when your cable provider was offering the "triple play" package? It consisted of ***bundling*** your phone, Internet and TV into one bill. How convenient, but so wasteful. In fact, cell phone service is good enough now, that people are getting rid of their landline service entirely.

You've probably noticed the number of people that are now "cutting the cord" on one of the other bundled services. That's the term used for people that are no longer subscribing to cable TV services. They instead, are subscribing to services like Netflix, Hulu and Amazon Video for their TV entertainment, just to name a few. Imagine the major impact on Internet providers. The bulk of the triple play cost is for TV and if people are cutting this, Internet providers are being forced to make up the revenue in other ways. Correspondingly, for those that cut the TV service and only subscribe to the internet package, these same consumers are faced with throttling their bandwidth speeds in order to replace lost income.

See where this is going? The Internet provider is losing a huge (TV) revenue stream, BUT they were just allowed to sell your browsing history without your consent, courtesy of legislation SJR-34.

11. Private from who?

When a browsing solution tells users they keep you private online... ask them from who?

Here are some other pertinent questions to consider as well:

Do they keep you private from other users of **your device**?
Do they keep your browsing private from the builder of the **browser being used** (Google, Microsoft, Apple, Mozilla etc...)
Do they keep your browsing history private from the **Internet provider being utilized**?
Do they keep you private from **every website** visited?

Looking back on the FOUR points of browsing, MANY browsing solutions claim to be private if they keep you private from just ONE of these FOUR points. There's really ONLY ONE solution that does this for all 4 points though!

12. Besides Search and Youtube, THIS is How Google Knows so Much

Any company or website that takes their ecommerce/search ranking seriously, wants to know how traffic got to their site and any methods that can be used in getting more traffic to their site. Consequently, they do this by placing free computer script (cookies) from Google and Facebook on their site. This gives a website LOTS of information about each user...namely, what time they landed on the site, how long they were on it, what pages they looked at, the location of the user,

what OS (Operating System) their device uses, what browser they used, their IP address, what site they came from, what keyword was used to find the site, how many times they have visited the site before, what pages they visited on the site and for how long.

Readers might ask, just how do they know all these things? Let's say you use Orbitz to search for a flight. Orbitz then places a cookie on your computer. A cookie is a small file that basically says "I want to find and know about flights to Europe". Orbitz can then sell that piece of information to big data companies. These big data companies auction it off to the company with the highest bid. In this case, say a major airline like Delta. Once they know what kind of flight you're interested in, Delta then shows you ads for relevant flights... NOT JUST on Orbitz's site, but on ANY site you visit, and on ANY of your devices. This whole data collection and sale process takes under a second!

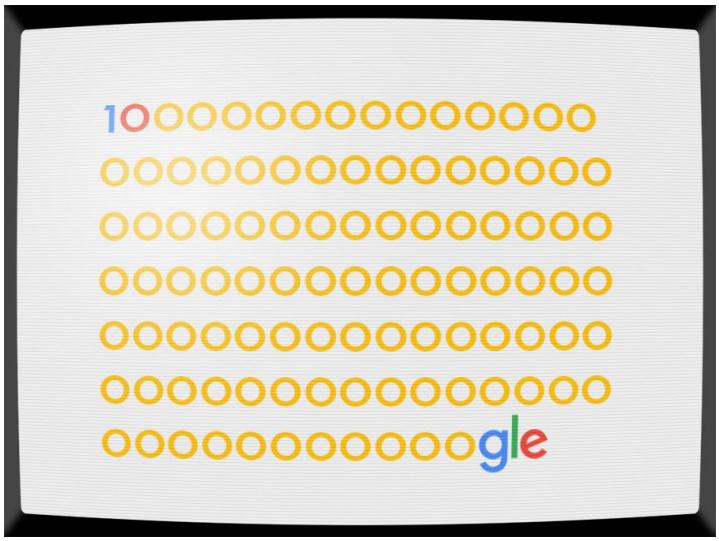
What this means, is that companies can reach you AFTER you leave sites that relate to their business. You can see airline ads when you're on a sports or news site. You wouldn't let a sales clerk follow you around the mall, or certainly after leaving it would you?

All of this information is aggregated and found with many web analytic services, but the biggest one by far is from Google called *Google Analytics*. Approximately 80% of all websites have tracking scripts on them. Knowing this, it's no surprise Google generates the bulk of their revenue from delivering relevant ads and search results based on the user. Obviously, the more information they can gather about the user, the more targeted ads they can deliver to that person. It stands to reason then, cookies ONLY have value if they can **correctly** identify the user. However, if an Internet advertiser places ads targeted to a person that really isn't that person, they are not relevant and the ads won't be clicked on.

The HUGE business of matching these people together, called *search engine optimization,* is the act of making this happen efficiently and Google thrives on this!

One of our favorite books, *The Googlization of Everything* **(book link)** by Siva Vaidhyanathan is most apropos here with this quote: ***"Google measures us and builds its systems and services to indulge our desires and weaknesses".***

13. It was Originally Called *googol* For a Reason



(source)

What the heck is a googol?
Well Google, the now gargantuan popular search engine, was originally called googol. This was because a googol is the large number 10^{100}. In decimal notation, it's written as the digit 1 followed by **one hundred** zeroes.

Needless to say, that's a heckuva lot of information.

So how does Google follow you? Let us count the ways.

Do a Google search, visit any of the 85% worldwide sites with Google Analytics on it, such as playing a video on Youtube, looking at a Google Map, opening/sending/responding to a Gmail, deploying the Chrome browser, utilizing an Android phone, using Google Translate, Contacts, Finance, News, Shopping, Zagat, Waze, or do one of those annoying Captchas etc...

Each time you use one of those services, you're giving Google information that will NOT be kept confidential.

Here's another thing to consider. Each time you use one of the above forms of Google, that activity is immediately shared across EVERY device you have ever used with Google.

When people say they don't use Google because they want their online privacy, well you now know that's virtually impossible. To that end, another excellent quote we love from *The Googlization of Everything* is, ***"Google is the lens through which we view the world".***

Users cannot help BUT USE some form of Google when online, and device(s) used are LOADED with pieces of info that Google can use to identify them and their browsing. More specifically, YOU and your browsing!

14. Incognito or Private Mode

(source)

Incognito: *having one's true identity concealed*

Probably Google's biggest coup, was introducing this mode on their Chrome browser called *Incognito*. This was supposed to let users think they were incognito when browsing. Give them a ton of credit, because it took 10 years for the market to **finally** realize it isn't private at all! As a consequence, the majority of the population has been sharing their private browsing with the world's largest data gatherer. Pretty sweet gig if you can pull it off!

This is right from Google's website and what they consider "incognito" mode:

When you browse privately, other people who use the device won't see your activity.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode.

Your activity might still be visible to:

Websites you visit, including the ads and resources used on those sites
Your employer, school, or whoever runs the network you're using
Your internet service provider

As one can see, you do NOT conceal your identityl… hardly incognito at all, but MILLIONS of people use this mode every day thinking they are private! Do you really think for a second now, that Google is going to tell them they aren't?

When you use *Incognito*, your device and browser continues to shake hands with every website you visit. The ONLY browsing privacy you get, is if someone else uses your device, they cannot immediately see your browsing history. Unfortunately, if they are tech savvy enough, they can STILL figure out what sites you visited!

In following the tech bell cow called Google, ALL the major browsers now have some form of "private mode", which really isn't private at all either.

What follows is a brief explanation of another kind of "Private" browser.

15. "Private" Browsers

At this point we need to make a distinct differentiation concerning quote, unquote *"Private"* Browsers. These are not to be confused with using your regular browser in *private* or *incognito mode*. *"Private"* browsers are simply browsers specifically built to run only in "private browsing mode", AND they block ads OR website trackers. In fact, they are NOT private (or secure) at all, because your device STILL connects with the end website! Therefore, ANY website visited using these type browsers can identify you, and the cookies on your device. Not only that, because the website shakes the hand of your device, you can get viruses as well. And yes, you guessed it, your Internet provider (IP) can also see the sites you visited too.

Even with these so called "Private" browsers, you will notice when it comes to their supposedly "private" browsing solutions, ALL (regular and private browsers) have the same thing in common. The browser is always running on the device… and the device(s) always give you away. Not just

the one you're browsing with, but the ones using the same "pipe" internet signal IP address… again, that includes the one in your pocket.

16. Private Search Engines

2 + ? = 5

The next farcical myth on the list, is that a "private" search engine keeps your searches private.

Looking at the above equation, a private search engine is basically saying they will not share **?** with anyone. In addition, they state all **?**'s won't be stored in their database. Some private search engines will even say they use different types of **?**'s, or that we hide the **?** Quite ridiculous isn't it, considering the simplicity of the equation? But hey, it sounds pretty good, wouldn't you agree?

Search the Web with a free private search engine and it won't store or share your search queries. Private search engines work exactly like big Google or Yahoo search engines! The exception is, they don't gather, store or process any information about you or your searches.

Here's the reality though. The device (and probably the browser) used on a private search engine is LOADED with Google cookies. Chances are you came from a site with a Google cookie on it, and the search result you clicked on had a Google cookie on it too. Face it, the company that has mastered how to get information from any user on the Web, can certainly figure out this simple algebra equation!

There's a really good quote on one of the leading private search engines which neatly sums up what really happens.

"*We don't track you but others do"*. Now, when they say "others", they are referring to other search engines like Google. However, here's the thing if you are using a regular browser and your device, there are enough Google cookies on it to realize what searches you made. Your search history is NOT private from Google, even when using these so called private search engines. Simply stated, your device which has all of these cookies on it, touches the end site most likely with Google script on it too!

Something else to consider here, what do you usually click on when you do a search? Well, usually sites on the first page, like most everyone else. By the same token, if they are on the initial

page of a search result, there's a very good chance this first page uses Google Analytics. So between your browser, your device and the sites landed on, Google can figure out LOTS of things. Namely, who you are, where you came from, and what you were searching. Even if your private search engine says they don't share (or they encrypt) your search queries, they can **still** be identified.

Did you know the Chrome browser, which is used by almost 70% of the world, **is owned by Google?**

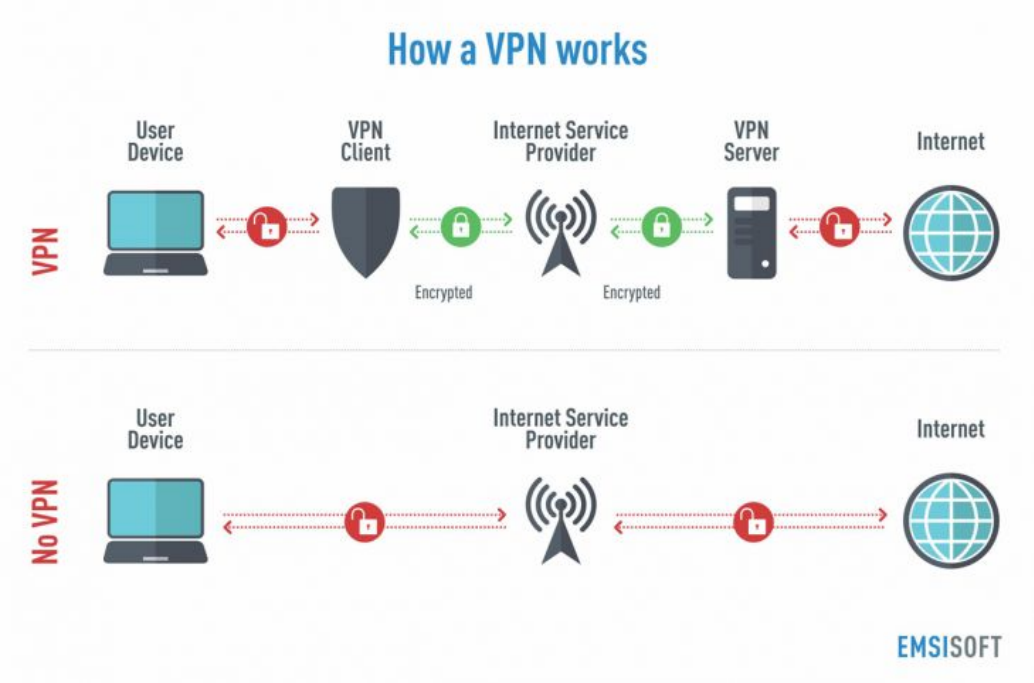
With this in mind, all you are really doing when using a private search engine, is getting subpar search results and letting Google know you tried to be private when performing a search. If you feel better using a private search engine fine, just know that your devices are LOADED with Google cookies. Google can **still** tell what you searched for and what sites were visited, because your device is still shaking hands with EVERY site you visit. In like manner, users are in fact digitally greeting every site visited with their devices, so all the websites know too.

Hopefully readers can see why Google has never bought a "private" search engine? They don't need to!

At this point in time, because we only briefly touched on VPN's (Virtual Private Networks) earlier, a more in depth discussion is now warranted.

17. VPN... Virtual Private Network

"Commercial VPN is an over glorified fraud for sake of cashing in the privacy hysteria" (source)



(source)

(see our earlier explanation of a Virtual Private Network in *Key Facts About Encryption and VPNs*)

VPN technology came out around the same time Windows 95 was launched. We know what you're thinking, hardly next generation technology! Today, they are being promoted to people without technological knowledge as a way to surf the Web privately. In all fairness, up until now there hasn't been a way for the CONSUMER to surf securely, let alone privately. Recall our earlier discussion about the FOUR points of browsing? Well, here's the real problem with using a VPN. They only provide privacy with ONE of these four points of browsing...namely, the *Internet provider*. You are not private (or secure) on the other three points *device, browser and website.*

Looking at the simple diagram above and one can see, your browsing data is unlocked where the locks are red, along with where it reaches the Web and as it reaches your device.

Here's all you need to know about using a VPN

During the round trip of visiting a website, your data is locked and unlocked, along with then being locked and unlocked again. As you can imagine, this makes your browsing VERY slow!

ONLY data that you type and send is locked, NOT the data on your device.

With this in mind, your data is only locked when it passes through the Internet provider. It's then unlocked when it reaches the website, which makes locking it kind of useless.

Useless, because your device still interacts with websites, meaning they can **still** identify users by their device and the information on it (true location, cookies, etc...)

“Locked” data does NOT mean the data is safe, it just means it’s concealed or disguised, so the provider can’t see it. It does NOT mean it’s necessarily safe to open!

Additionally, there are some other things to know when using a VPN. Your device touches the website, so the website can see the cookies on your device, which gives them A LOT of information about you. Not only that, but they can also place cookies on your device and then track you online. If you’re lucky, the site will only leave cookies on your device. Then again as we have shown, because the site touches your device, you are ALSO vulnerable to viruses. Your browsing history is left on your device too, letting anyone who has access to the device, the ability to see where you browsed.

So the next time you hear the term encryption being used, realize it just means the data is being put in a box so others can’t see it. Reiterating here, it does NOT make the data safe to open!

While you may just now be hearing about them on the news, as a way to browse the Web privately, the VPN is really considered antiquated technology! Where *Incognito mode* was long hailed as being private (but still only covered **one** point in the FOUR points of browsing), now VPN’s are being promoted as being private. In the same fashion, they too only protect **one** point in the browsing chain (Internet provider). Please don’t make the same mistake again, and fall for the “log policy” ploy either!

Log policy

This is basically a record of what sites each user visited while using the VPN. Readers will see this advertised a lot in the VPN world. In fact, some VPN’s try to convince users they’re private with them because they don’t keep a “log policy”. Again, here’s the real deal. Regulatory agencies can identify you by the following:

1. If your device is in the U.S.
2. If the website site you visited is in the U.S.
3. If you traveled using a U.S. Internet provider/telco

Don’t think for a second you’re hiding your Internet activity because the VPN being used doesn’t keep a “log policy.”

Reiterating here, Virtual Private “Network” is a complete misnomer... there really is nothing private about a network!

Above all, the one thing you must take away from this:

A VPN only secures your data, it DOES NOT secure or privatize your device.

Readers are are probably seeing a veritable plethora of ads for VPN’s now. Some are even offering lifetime subscription rates. The real fact of the matter is simply this, the antiquated VPN is on its last leg and market leaders are trying to capture every last dime before the inevitable shift to cloud browsers arrive.

Before getting to our next browsing solution, we should take a brief moment and explain what the “Dark Web” is.

18. The Dark Web

(source)

The Internet is massive. Millions of web pages, databases and servers all run 24 hours a day, seven days a week. But the so-called "visible" Internet, sites that can be found using search engines like Google and Yahoo, is just the tip of the iceberg. Below the surface is the Deep Web, which accounts for approximately 90 percent of all websites. The “Dark Web” then, is classified as a small portion of the Deep Web, that has been intentionally hidden and is inaccessible through standard web browsers. In fact, this hidden Web is still so large, that it's impossible to discover exactly how many pages or sites are active at any one time.

The Dark Web is a term that refers specifically to a collection of websites that exist on an encrypted network and cannot be found by using traditional search engines like Google and Yahoo, or visited using traditional browsers. This Dark Web was once the province of hackers, law enforcement officers and criminals. However, new technology like encryption and the anonymization browser software, TOR, now makes it possible for anyone to dive deep if they're interested in associating with this **“dark”** world.

Additionally, almost all sites on the so-called Dark Web hide their identity using the TOR browser.

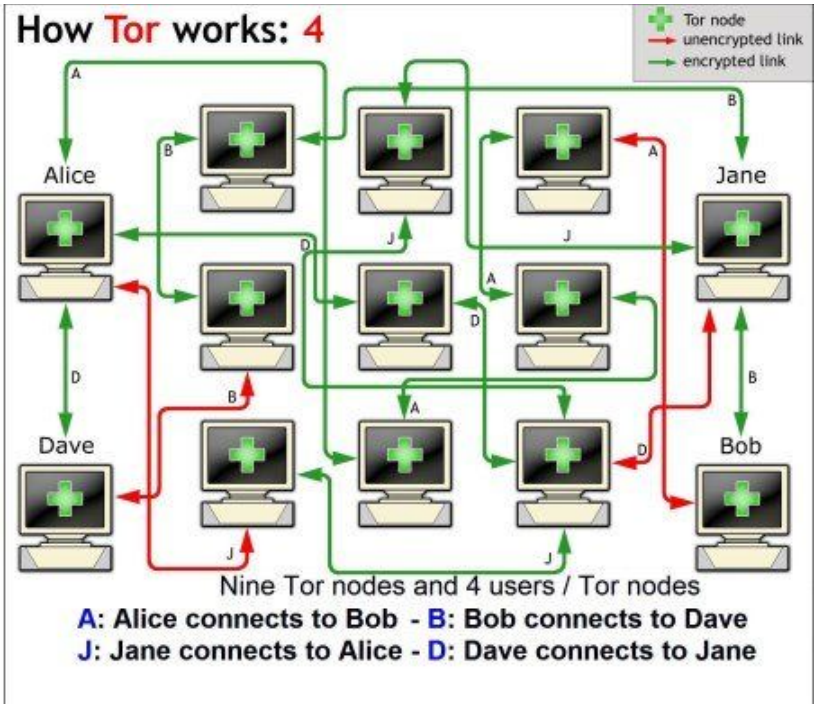
It’s called **“dark”** for a reason. This is NOT a place to surf with an unprotected device.

With that explanation out of the way, let’s take a closer look at this TOR browser software.

19. TOR

Tor is a web browser software that conceals users identities when they're online. It does this in a few different ways. First, it uses encryption to scramble the data that's being communicated within the network of people like you, hiding their browsing. Second, it routes your data between random computers (you do not know) within the TOR network to hide your online identity, including data tied to your personal IP address. People are always looking for the “new thing” and TOR is getting more popular as privacy becomes a concern. As previously stated, the Dark Web is where the bad guys hang out!

Now, there are some really nasty and negative results from using this technology. Not only is TOR incredibly slow because your data has to pass through all those strange computers, but the network is widely known for sharing content that includes child pornogrpahy, human and drug trafficking, murder for hire and a bunch of other goodies. Oh yeah, bad guys like to hide nasty viruses in the content on the Dark Web too. With that, let’s take a look at the following diagram:



(source)

What do you notice first? Well, look at the number of strange devices you must touch in order to reach your final destination. Not only is this browsing incredibly slow, but in the process, your device “touches” other devices trying to hide their browsing.

Certainly, something you need to consider. Imagine that YOUR BROWSING is going through an IP address that is/was doing something illegal! On the flip side, what if illegal activity was going through your IP address?

We have just one piece of advice, if you are not doing anything illegal, **DO NOT** use TOR.
Then again, if you want even more reason NOT to use TOR, please visit this link

20. Free” WiFi

When you access the Internet using a WiFi hotspot (free or not), this lets entities like Starbucks, the airport and hotel etc... put a tracker on your computer or device, along with then following you when browsing!

Some of the larger establishments will either show you their privacy policy, or just make you accept it before allowing you to surf. Obviously, you’re there for the free Internet, so who bothers to read it

anyway. We will however, show you later how to hide your browsing from a WiFi provider and prevent them from tracking you.

Getting back to using a WiFi hotspot, just because you're using someone else's Internet, does **not** mean you're private. Likewise, did you know that even when you disconnect from the WiFi, their tracking code stays on your device?

21. Ad Blocker, Cookie Blocker and Do Not Track

Ad blockers are nice because they remove... well ads. Not only do they make surfing more enjoyable, they also speed up the loading of the site. Although this may be true the vast majority of the time, blocking ads does **not** make your browsing private. You run them in your browser, which runs ON your device.

Let's talk about cookie blockers. There are plugins to your browser that claim this. But be that as it may, there are also applications and sites that claim to block cookies from getting on your device. They may stop a few, but they don't stop them all. Once again, they run on your browser, which runs ON your device. Are you seeing a pattern here?

Chances are, you downloaded one of these apps through an app store too. If you feel better using one, go right ahead, but the smartest geeks **still** know how to place code on your device (and replicate it before you even know it). Of course, your device **still** shakes the hand of the website with these too.

The *"Do Not Track"* feature that some browser's offer, has also been proven to be useless.

If you haven't figured it out yet, there's no way you can achieve complete security and privacy if your device shakes the hand of another computer, or simply put if the browser runs on your device. Apps, extensions, private sites, special browsers don't mean diddly if the code from a website is executed on your device.

Let's now shift our focus to anti virus software.

22. Antivirus… Does NOT Mean Virus Free

Anti virus simply means software designed to **detect and destroy** computer viruses.

This is very much like the difference between *resistant* and *proof*. Do you want a solution that is virus resistant or virus proof? The biggest corporations in the world, who spend millions of dollars for online security are getting hacked! Do you really think you're smarter than their IT department, or the bad guys?

The new viruses coming out are more secretive. They stay hidden and record EVERY keystroke you make. Correspondingly, EVERY time you type a password or a credit card number, this is seen and stored.

Just imagine the Internet as an alligator filled lake, and you use a boat to navigate the lake. Of course, antivirus players will tell users they will protect you and your boat from any alligators. They detect and destroy any alligators that try to get in your boat. That's great, but consider the following questions:

What if your boat gets a leak?
What if there is a massive downpour?
What if your boat hits a hidden stump?

There are new ways that your boat can be compromised every day. So, rather than try to use YOUR boat to navigate a lake filled with alligators, wouldn't it be smarter and safer to use a remote controlled boat?

You can subscribe to the latest antivirus service, add a firewall to try to protect your device, or just use what the Department of Defense and many financial institutions are incorporating. Namely, using a virtual machine (ie a remote controlled boat). Virtual machines are an isolated environment from the physical operating system, so you can run potentially dangerous stuff such as malware, without fear of compromising **your device.** They're a **safe** environment for browsing, and we will discuss these next.

23. Virtual BrowsING and Virtual BrowsERS

The top research groups are now saying that browsing in the cloud IS the future, although you won't hear your local news anchor talk about yet. We don't want to lose you here with this high technology discussion, so we'll do our best to simplify it.

Virtual browsing is a service that uses a **regular** browser (Chrome, Firefox, Internet Explorer and Safari) on a virtual computer (virtual machine) in the cloud. The browser runs in the cloud (NOT on your device). Your device (keyboard and mouse) act like a remote control to the computer/browser in the cloud, and ONLY what the computer "sees" is transmitted back to your device's screen, **not** the code.

Only the virtual computer and browser in the cloud interact with the website, NOT users' devices. All links are opened in the cloud, with the virtual machine keeping your device safe from any viruses. Basically, users are renting a computer in the cloud to surf the Web.

A **virtual browser** is usually a proprietary browser that runs on a virtual machine.

Imagine putting on a virtual reality headset and experiencing SeaWorld. You're in the front row of the Shamu show. The big killer whale lands right next to the glass and water flies at you. It's so real you turn away. The cameraman that took the footage probably got wet that day, but you don't get wet. Instead, you get the awesome experience of being there without the physical effects of getting drenched. THAT is virtual browsing!

When users surf the Web with a virtual browser, they get to see what the computer and browser in the cloud are seeing without any "water" ever touching their device.

Major financial institutions are backing this technology now, and the Department of Defense just issued their cloud browser strategy.

Due to the cost and complexity, virtual browsing services have only been available to commercial and federal enterprises.

Virtual browsers are also called cloud browsers, remote browsers or isolated browsers by tech experts. If readers want technical explanation of what a virtual browser is and how it runs on a virtual machine, they can read it here.

24. The ONLY Virtual Private Browser

This is a combination of private AND secure browsing. It's a completely secure and private browsing service. Each time a user logs into the cloud, they not only get a "new computing device" (virtual machine), but they also get a brand new cookie free proprietary browser. Now, because both the computing device AND browser are brand new with each session, there's no evidence of past browsing.

The browser was built in such a way, there's **no** history during the session either. Not only is the user's true location hidden (the cloud provider's IP address is seen), but the browser is always isolated from the user's own computing device. Because of this, ALL cookies, viruses and browsing history are attached to the computing device in the cloud and are deleted on logout. As a result, this data NEVER gets on the user's own device.

The user is both completely secure AND private while browsing! The best way to describe this is, the computer in the cloud opens the “package”/website/file, and **not** you or your device. Websites only see the IP address of the cloud provider, the device’s specifications and the browser running on it. The Internet provider **cannot** see what sites the user visited and therefore **cannot** share this information.

In effect, websites see a “passport” that has no identity! They can see where the user went, but they CANNOT identify who the TRUE owner of the passport is. Not only that, but with each browsing session, users get a brand new identity free passport.

There are 6 points in this solution and they are as follows:

1. The device (which is your mouse, keyboard and screen)
2. The Internet provider
3. The server in the cloud
4. The virtual browser
5. The cloud provider
6. The website

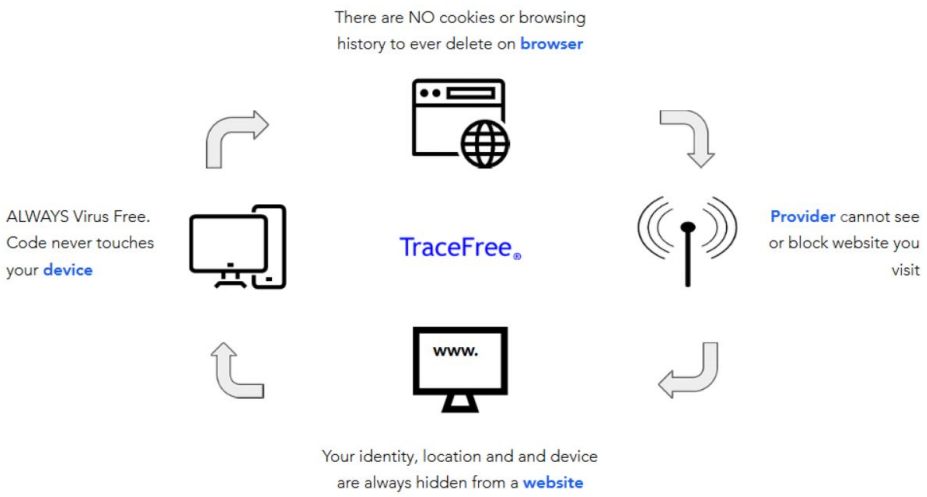
Out of all 6 points, the ONLY point in the cycle that can identify the user is the TraceFree server in the cloud. That data is NEVER sold or shared, much like a Swiss Bank.

There’s NO TRACE on the user’s device OR on the virtual browser. The Internet provider cannot see where the user surfed, and the cloud provider can only see the sites the user went to. Because of this fact, they CANNOT identify the user! Users of TraceFree call it a ***“disposable browser”***.

So while you cannot eliminate cookies from getting on a device, you can use someone else’s computer from a different location.

Other virtual browsers are available to enterprise or Federal employees, but TraceFree, is the ONLY virtual PRIVATE browser now available to consumers!

You can subscribe today here



Does the following describe you?

As a lifelong Internet surfer who became aware of Google's *Incognito*, along with various other privacy browsers and solutions, actually thought I was private, secure and safe using them! Needless to say, after reading all the above, nothing could be further from the truth!

However, NEW technology has arrived. The aforementioned Peter Steiner's original cartoon has come full circle. In that a way to browse the Web as a dog, has indeed arrived again, therefore giving way to a new image for the Internet. Look no further than our boot wearing TraceFree dog, surfing the Web without a care in the world, when it comes to privacy, security and safety!

Our TraceFree dog (YOU), can now leave their finger/footprints all over the Internet, but they can be deleted without a speck EACH and EVERY time they choose to take a stroll/surf on the Beach/Web.

We can't emphasize this enough. ONCE AGAIN, thanks to new TraceFree technology, Big Tech can't tell if you're a dog on the Internet!

YOU CANT HIDE YOUR DIGITAL FOOTPRINTS, BUT YOU CAN WEAR SOMEONE ELSE'S SHOES.

25. Secure, Private and Unbiased Browsing

Each session begins with a brand new cookie free browser. There's no browsing history to be profiled with, because you have a disposable browser EACH and EVERY time with TraceFree.

Because you are surfing with a virtual machine in the cloud, each site you visit doesn't know your true location and they cannot touch or identify your device. That simply means you are completely anonymous and secure on EVERY website. **ALL search engines used with TraceFree are private, and every search query is anonymous**.

All cookies and data generated during EACH session are deleted at the end of your session, TraceFree users have a true disposable browser! Not only can ANY data generated during your session NOT be associated to you, it is deleted on logout as well. This means, NO creepy ads following you ever again.

Furthermore, online pricing is unbiased, and therefore almost always the most competitive. Websites and advertisers have no idea you've been checking flight prices every day for the past week and what your online buying habits are, so they have no reason not to reveal the cheapest flights.

While users can't erase their previous browsing history pre-TraceFree, you can anonymize (and delete) it (moving forward with TraceFree). Think about the benefits, your future browsing won't be impacted by your previous browsing!

Your Internet provider will never be able to see what sites you visited or searches made. The peace of mind knowing that your boss, credit card issuer, competitor, insurance company, lawyer and dating site (to name just a few) can NEVER discover where you went online and what information you shared or requested, is incalculable.

Equally important, users can always click on any link without wondering if it's a "bad link" or not. You won't have to update your antivirus program.

You can know with certainty that any search or news is delivered unbiased.

We like to think of TraceFree as having a “Swiss Bank Account” for your browsing. User’s browsing exists with one isolated entity and it is matched with a unique number, **not** a name. With **each** and **every** browsing session, the user gets a brand new browser with a 15 plus alphanumeric digit. Think of it with this global scale deli analogy, in order to identify the user, someone would have to know the following:

In what country
In what state
In what supermarket chain
In which location
What time and number did they pull at the deli counter

Just like when ordering some bologna, the number is thrown in the trash after the service is rendered. Certainly a monumental task for anyone wanting to discover a customer’s, or in this case a browser’s true identity! Only with a government agency or law enforcement request, would your browsing ever be disclosed.

Yes, there ARE times when you want personalized assistance from a librarian, clerk or a search engine. On the other hand, we all know there are times when you don't want to call attention (have their opinion, or that information sold or shared) to what you are looking for or want to buy.

26. One Simple Trick

There’s an easy way to tell if you’re private and secure online. Can you upload a video to Youtube, post a picture on Facebook or attach/open a document in an email? If you are able to download, upload or attach any content, then your device is able to “connect” to another computing device. Consequently, the realization is, you are not secure and certainly NOT private! That simply means your computer CAN touch another computer. Your anti virus program blocks or scans any incoming files, but it **still allows** a connection to the other device. It may not allow the visitor to enter, but it opened the door to see who it was. Regrettably, that’s sometimes all it takes. Putting it another way, it simply means it’s possible for your device to touch another, and that’s all it takes to lose your privacy and not have security. It’s also the difference between virus resistant or virus proof.

When using a virtual private browser, it’s like having your packages sent to another location other than your house, and someone at that location opens the package... never you! In these cases, you and your device are ALWAYS isolated from the package. In light of this differentiation, let's take a look at the evolution, along with the pros and cons of the browser. Of course, green meaning safe, and red unsafe in the below:

The Evolution of the Browser

- **Browser**
- **VPN (using encryption with a regular browser)**
- **Browser in Incognito/private mode (regular browser that doesn't store history on browser)**
- **Private browser (browser that runs in private mode or blocks ads)**
- **Virtual browsing (regular browser that runs in the cloud)**
- **Virtual browser (proprietary browser in the cloud)**
- **Virtual private browser (disposable proprietary private browser that runs in the cloud)**

Shakes hand with website/computer (UNPROTECTED BROWSING)

Doesn't shake hand with website computer

27. Finally Your OWN Privacy Policy

The purpose of this book was to educate the browsing public about the evolution of private browsing, myths associated with it and the resulting negative consequences resulting from data aggregation by Big Tech and others, along with the potential harm to all users devices that are connected to each other.

Taking all the above into consideration, the experts said to use Incognito mode and they were dead wrong. Now, "they" are telling you to use technology that is over 20 years old (VPN). Well, as we have pointed out earlier, wrong again!

The Department of Defense and major financial institutions, are now switching to browsing in the cloud for security. In like manner with TraceFree, because users are browsing in the cloud, they automatically get the same security. However, equally as important using TraceFree, you also get complete privacy too!

After years of having websites identify and track users online, **YOU** get to choose if you want to share **ANY** information with a website.

Now, the proverbial shoe is on the other foot. Rather than wonder what information each online party is getting from us (and what they are doing with it), we make our very own **PRIVACY POLICY** possible! By default, **NO** information is given out unless the **USER CHOOSES** to do so when using TraceFree. In effect, there are no privacy settings to update or decipher. In addition, **NO** cookies or browsing history to delete. Here's the real kicker about this revolutionary technology, there's no need for Opting -Out, because you NEVER Opted-In!

For the first time ever online, **you have** the power over Big Tech, by simply having the choice of Opting-In, versus **always** trying to figure out how to Opt-Out.

There's now a way to use someone else's "shoes" when you browse the Web. As a result, **YOU CAN** completely hide your identity, location and device when surfing. We can't state this strongly enough, for the first time ever, you the consumer have your **OWN** privacy policy! More importantly, your personal privacy policy trumps **ANY** website's policy… **take that Big Tech!** It doesn't matter what information they get from your visit, because it isn't yours! With TraceFree, you have ALL the power, and can choose not to share **ANY** of your information when you browse the Web. What a revolution….**THE TraceFree Revolution!**

For speaking engagements, interviews or for more information please contact us at:
info@tracefree.com

BONUS SECTION

TEN Ways To Know If You Are Private & Secure Online

1) The browser you use, did it come preinstalled on your device?

Remember when you were so anxious to start surfing the Web? You opened the box and immediately started using the browser that was installed on the device.

However, upon purchasing the device, your credit card information, email and physical address were provided to the manufacturer and merchant. In fact, this information was automatically sent to the manufacturer and then used to register the device, along with ALL applications installed on it. Every computing device has a unique identification number.

2) Is the private browser you downloaded free to use?

You're a smart consumer and informed about the many ways you're being tracked online. Wanting to escape the clutches of Google, you went ahead and downloaded one of those "private browsers". This begs the question, is that browser really free to use?

Well, you know the old saying, "if you're not the customer, YOU ARE the product". There's nothing free in life, and especially on the Internet.

3) Can you download, upload or attach content from your device to a website or in an email?

Actually, this is probably the easiest way to tell if you're completely private and secure.

Can you upload a video to Youtube, post a picture on Facebook or attach a document in an email?

If you are able to download, upload or attach any content, then your device is able to "connect" to another computing device... meaning you are not secure and certainly NOT private.

4) What happens when you visit your favorite sites?

When going to your favorite sites, are you required to login, or are you automatically logged into the site? In addition, when checking your email (Gmail, Yahoo, AOL), do you need to log in every time?
If automatically logged in when you visit these sites, they can recognize you by the cookies on your device. It also means other sites can identify you as well.

5) Do you need to clear your cookies and cache?

Cookies... they are little pieces of code that are attached to your browser and device when you visit a website. Some are very useful because they help a website identify you when visiting them. Other types, also called 3rd party cookies, are used to track and identify your browsing.

If you have never cleared your cookies, then it's safe to say that you're an advertiser's dream for giving them so much information.

If you do clear your cookies, have you ever noticed that several automatically still appear when you restart the browser? This is because they are 3rd party cookies that just cannot be deleted. Kind of frustrating to know isn't it?

6) When a website asks you to enter an email address or username in a form, does your browser auto fill it in for you?

Of course, remembering website passwords is a pain. Knowing that, browsers now make it easy to remember your password by filling in this info for you. However, this info IS STORED on your browser, which can be VERY dangerous if visiting malicious sites.

7) When you visit your banking website, are you asked EVERY TIME to verify your identity with either a text message or confirmation email?

Almost all financial related websites now require a second type of verification when they don't recognize the device and username. If you are not required to do this when logging into your bank site, it means they can easily identify the device. If they can identify you, so can other sites you visit.

8) When you start typing in a web address does the browser autofill or auto suggest the website?

Typing in web addresses can be a real pain. When you start typing a URL in the address bar, does the browser autofill or autosuggest it for you? If so, your browser is basically saying "*we know where you usually go, and WE WILL take it from here*".

9) Can websites correctly identify your browser?

First determine what browser and version you are using. Go ahead and open your browser in incognito mode or private mode, and then visit www.whatismybrowser.org
Is that your browser? If that site can identify your browser, it means a website (computer) can "touch" your computer in order to identify it. In effect, when a computer/server can touch your device in this manner, it means they can place and read cookies on your device.

10) With your current device, have you ever logged into Google, Facebook or Amazon?

It's almost impossible to say no to that question. Google and Facebook are extremely good at reproducing your browsing activity across ALL the other devices you use online, INSTANTLY. Deleting your activity on one device does NOT delete it on the other devices you use. In fact, as soon as you use one of the other devices, this history shows back up. It's a game we call "Wack a Cookie". Think about this for a moment, have you ever done a search for an item and then have an ad show up on another device?

There's a great reason Facebook and Google are able to deliver such targeted ads and own 90%+ of the Internet advertising industry.

Here is how a TraceFree User answers the following questions

1) The TraceFree Browser is downloaded from the Internet. It's a thin client app that basically connects to a server in the cloud. Nothing (cookies, browsing history or viruses) ever gets stored on your device.

2) Virtualizing an application in the cloud isn't free. TraceFree charges roughly $5 a month, so that you can browse with complete security and privacy.

3) There is no possible way to download, upload or attach any content when using TraceFree. The browser runs in the cloud and your device NEVER touches a website. On the flip side of not being able to share content from your device, it also means it's impossible to download any bad viruses and websites cannot access it either.

4) Visiting your favorite sites will require you to provide username and password. This may seem like a pain, BUT this is a very small price to pay for true privacy and security.

5) Each browsing session with TraceFree is with a brand new cookie free browser. All cookies that you collect while browsing are deleted on logout. You NEVER get cookies on your device and never have to clear cookies when browsing.

6) With TraceFree, you will find in all entry windows for an email address or username/password, that the browser doesn't autofill it in for you. Remember, you always start your session with a brand new browser and it has no memory.

7) When you use TraceFree, financial websites WILL NOT recognize the device you are using, and WILL ask you to confirm your identity with another method (SMS or email). While this may seem like a pain every time, it's actually a very good thing for you. It means your device is not giving away or storing this information on your device. True security and privacy.

8) When you start typing in the address bar, quickly notice that it doesn't autofill a web address or make suggestions. The TraceFree Browser has no memory. This simply means NOBODY can tell what sites you visited.

9) When you use TraceFree, you're really using a separate browser in the cloud on a virtual machine, **not** a browser on your device OR your device itself. If you visit www.whatismybrowser.org the site will identify THAT browser, and not the ones on your device. This way, you are anonymous and secure on any site.

10) One of the really neat things about using TraceFree is the ability to control the info you give to a website. Of course, if you want to use Google Search within a TraceFree session with complete anonymity, you can! However, if you want to login to Google inside or outside a TraceFree session and reveal your identity, you can do that also. Remember, with TraceFree you are ALWAYS anonymous on a site UNLESS you choose not to be by logging in… At that point YOU give away your identity.

For speaking engagements, interviews or for more information please contact us at: info@tracefree.com

Recommended reading:

The Filter Bubble What the Internet is Hiding From You by Eli Pariser

The Googlization of Everything (And Why We Should Worry) by Siva Vaidhyanathan

Algorithms of Oppression How Search Engines Reinforce Racism by Safiya Noble