The Paranoid's Bible

Non-profit and free for redistribution
Written on June 04th | 2014
Published on October 22nd | 2015

For entertainment and research purposes only

DISCLAIMER

The Paranoid's Bible and its writers hold no responsibility for the acts of others.

The Paranoid's Bible is for research and entertainment purposes only.

Please visit our blog for more PDFs and information: http://www.paranoidsbible.tumblr.com/

Table of Contents

Preface

The who:
People that have decided to combine their resources to create a repository of information.

The what:
The Paranoid's Bible: A free to use resource that aims to help people self-dox.

The where:
The internet: An abused form of communication, education and betterment of mankind.

The why:
To give people the tools to self audit.

A History of Doxing

[1]Doxing is a term believed to have roots in the age of the BBS.

It describes the action of finding information on a target from an initial set of data in the form of a screen name or email. Many people find this information through search engines or other services offered online.

Take note that doxing can take place anywhere, even offline. Individuals can and will try their hand at social engineering. They'll do this by asking businesses or groups for more information on a target. It's accomplished through the claim of being someone they're not or through asking questions.

The word comes from 'document tracing,' which has a past in web 1.0.

Regardless, doxing's a neutral act that is free of political and moral responsibilities. It's used by many groups and individuals that range in religious and political beliefs. So, the person commiting the act is the one that places political or morals onto it.

The target can range from possible racists or sexists to an innocent person or a victim of some scheme.

Remember: Anyone can become a target and victim of doxing.

The truth is that no one is un-dox-able.

It's speculated this is the end result of mob justice and social justice on the internet.

Doxing is just something that won't go away. And just like its rise to infamy in the early 2000s, it'll always have its ups and downs. We just have to learn to co-exist with it and guard ourselves.

- Clarification on the spelling of Dox – One X only, not two. Dox is the proper, original spelling.

Resources:
What is doxing and how does it affect your privacy?
Know doxing, protect yourself.
Wikipedia - Doxing
Social Engineering Wiki - Doxxing
Know Your Meme - Doxing
Urban Dictionary - Doxing

Weaponizing Dox

The internet is quite like a middle school's playground. It's filled with immature individuals void of any real emotional or mental maturity. Just like in middle school, and some higher education, gossip is common. People will use your past against you. They'll work on every tiny flaw and mistake to isolate you from others. And, like a lion singling out an ill gazelle from the herd, some people are quite opportunistic.

Though, we'll note that's where the similarities end.

People online, at large, have no means of coping with opinions or views that don't match to their own. They're so afraid of something of theirs being spoken badly of, that they seek to silence. Doxing is currently the most common form for silencing this supposed dissent. It's used to shame, blame and emotionally or mentally scar someone into censoring themselves.

This self policing on tone and content isn't something that many will see as a reason to prevent dox. Many will see it as a nuisance that'll not happen to them.

Why would anyone target you, right?

You don't matter, right?

You're right. You don't matter. You're just another pseudo-anonymous individual. That's why it matters, too, though. By being online, you're already a target for doxing. You frequent social media, the threats doubled.

If you dare speak your mind, entire legions of perpetually angry individuals see you. They're mad at you for existing. They're mad at you for simply being an individual with their own views and voice. You said something they deemed bad. Maybe it's a "Micro-aggression" or wrong think. Either way, you are just another bump in the road for them. They're on an endless jihad to wipe out anything that might "trigger" them.

They don't care about you, either. Your family and friends will be targets, too. They'll lay in wait until you're at your highest or lowest. It doesn't matter to them; they just want to make you into an example for stepping out of line.

The line will shift and change constantly, yet it matters not to them. They want to ruin you and yours. Your job will be on the line. Human Resources will be harassed continuously with emails and phone calls. Your employer will wake up to their own social media accounts blasted with comments.

And, again, you aren't truly the target but what they perceive you as representing. It could be anything, honestly. But, you should still worry nonetheless. We may have stated in "The History of Dox" that doxing is a neutral act—and it is—but it's being weaponized.

Why You Should Fear Doxing

Many believe doxing is something not to worry about. These people believe that by not posting their names, they're safe. It's just not that easy anymore as we're no longer a part of Web 1.0. We're in more danger than ever before when it comes to our privacy. This is due to the interconnectivity of Web 2.0.

You've things like tracking cookies, which is common knowledge. But how many users are aware of Facebook spying on its userbase and non-users alike?

What about the fact that Google and its services are connected?

The average users shouldn't worry about the above, though.

What will affect the average user is cat-fishing.

Cat-fishing, in some ways, is like doxing and identity theft. You use someone else's information and identity to masquerade as that individual. You then, as this individual, take part in what many refer to as a "romance scam". This can be to try and stalk someone, milk them of their money, or to gain trust to commit a more atrocious act.

Cat-fishing, although like doxing, isn't actually doxing nor the biggest possible threat. Doxing to many is just **[1]** pizza boxing and flooding a mailbox with **[2]** literal junk. There are also prank calls, theft of mail and many other acts that can, to some degrees, become worse.

The issue isn't that some use doxing a means to gather information for identity theft. It isn't just ruining your credit or stealing your money, either. There are some individuals out there who'll use doxing as a form of abuse.

It isn't the stalking or physical abuse you should worry about, but the mental and emotional abuse.

That stress alone can damage your less-than-mature victims.

This is why many should fear doxing in its current form. Web 2.0 isn't just pranks and unwanted food. It's now a form of vigilante justice or revenge. It'll be done by those who see themselves as fighting for social justice. They'll ruin the livelihood of many due to any perceived wrong. They'll continue their antics until the person they're targeting is destroyed.

- Pizza-boxing is the act of sending pizzas or other unordered food.
- By literal junk we mean boxes, junk mail and similar items.

Resources:
Catfishing
Dr. Phil on Catfishing
"Doxing is like hacking but legal"
FTC on identity theft
Identity theft
FTC's advice for victims of identity theft
An ID theft victim's story

Why You Should Care

Information is the new form of currency that transcends borders and time. It's used by both the governments and corporations of the world. Due to this simple fact it's not only a valuable resource but also an important one.

Personal data is sought after, regardless of your worth as an individual. You aren't the one they're interested in--your information is worth more than you. Even when dead, your information is valuable. You can remain apathetic about your information as no one needs to worry when they're dead. It's just that the truth is quite scary. While you read this, someone is organizing your information into a dossier and selling it as a product.

Corporations and government sponsored alphabet agencies are putting your information into lists and dossiers. These lists and dossiers rest in the dark corners of some data center in Utah.

Every like, tweet, snap and chat saved.

Every bookmark, account and login time noted.

They track everything you say and view.

It's just the government, nothing to worry about... right?

Well the government's known for ruining things you love; you should know this by now. You should be wary not of the government as a being but as an entity composed of individuals:

- An individual can track an ex-lover
- A group of individuals can target another group based upon their political beliefs
- A group can view your pornographic viewing habits and use it against you

The US government is but one of the major concerns for a person that's privacy minded. They not only spy on everyone, but they receive help from many corporations. These corporations make money off you and your information. They will buy, sell and trade with both the government and other corporations.

Sites like Been Verified, Smart Zip and Intelius will gather and place your data on not only their sites but sell it to others. Even search engines like Google or Bing have your personal information. These sites can have anything from your name to your address or even pictures of your house and vehides

It may seem like fear mongering and a lot of fuss about nothing, but your information is used for anything and everything. Anyone can find it now. No one can be too prepared when it comes to their privacy and personal safety.

The Need for Privacy

It doesn't matter if you believe in conspiracies or not, we're not here to judge. It's just that if there was an actual shadow group looking to control the world... then they've done it well. In the West, especially the US, fear is now law and so is the removal of freedom.

We're exchanging privacy for so-called security. The millenials recognized this early on and completely fumbled the ball. They prefer instant gratification and "karma culture" instead of personal responsibility. Their calls for government transparency were nothing but a forced meme.

We regurgitate the catchphrases and trends force fed to us on news feeds and dashboards. We wallow in instant gratification and the infinite supply of praise we can get from the internet. All this has done for us is made us blunt to the concept of having some dignity. We air out our business to any and all who listen in the name of acceptance and progressiveness.

What we're doing is making ourselves ignorant to the fact that our privacy is dying.

Without privacy, there is no security.

Why do we need privacy?

Why is it important?

Well, without a natural set of social graces and respect... we'll see what every country under a budding tyranny sees before conflict begins.

Knocks at the door begin and men demanding a simple task: If you see something, say something.

Think of the recent ads on TV and online, or look at the news-paper or even a magazine. They'll have the same thing to an extent—don't trust people who aren't on Facebook.

Look around you; we're now in a continuous state of fear.

We may soon see propaganda in our cities telling us to report people for not socializing the correct way.

This is why privacy is important and needed.

Resources:

Consumers should be able to opt-out of having data sold.
Who let the dox out?
Know doxing, protect yourself.

Compartmentalization and You

When it concerns information security, compartmentalization is the act of limiting access to information to persons or groups who need to know it in order to perform specific tasks. The concept originates from the military when handling "classified information" and intelligence applications. The basis is that if fewer people know the details, the less likely a mission or task will be jeopardized and be risked. This helps limit the chance that data could be compromised or fall into the hands of enemies.

This also explains the varying levels of clearance within organizations, like "TOP SECRET" or the highly restricted "TOP SECRET ULTRA".

Like a well-oiled military machine, one must treat their online life like a separate entity that's in no way, shape or form, related to their offline life. This is to prevent cross contamination of accounts and information.

One such example of compartmentalization in cyber security, for the average internet user, is never using the same username or e-mail address for an account.

Another example would be purchasing a subscription to a good, secure VPN to prevent your own IP and ISP from being detect.

One other example is the use of add-ons to sanitize your referral links and randomizing browser's user agent.

In the end, the best practice is to treat each and every account as a separate entity isolated from your other accounts. A new e-mail address, username, persona and style of typing will be needed for each and every account you create to prevent possible cross contamination.

Please remember these simple steps when creating your accounts:

- A different username
- A different e-mail address
- A different password
- Always ensure you never use real world information
- Always ensure your avatar and/or signature is of an image you've used nowhere else
- Where you can, use a P.O. Box
- Where you can, use a pre-paid card instead of your credit or debit
- Where you can, use a burner phone (pre pair cell) instead of your landline or cell number
- Use a word processor to double check your written content before posting
- Try to limit the use of words you most commonly use
- Try to limit your account's profile in what information you provide
- Try to limit your overall account count to 10 or less
- Never link accounts to each other
- Never publicly post e-mail addresses or passwords
- Never share or link your chat, instant messenger or social media accounts to people you don't trust
- Never use your real name, nor should you ever post your real world information

Find your Digital Footprint - Introduction:

Transparency for the sake of online socialization and interaction is a threat. This trend won't die anytime soon, mind you. There are many reasons for this, such as the alarming growth of social networks. You've also the demands for online passports or services like Klout.

It's obvious the need for privacy is in increasing demand, but the biggest setback for privacy is you.

All those accounts you made in your early internet years? They have most likely left a nice trail that many can follow and use to learn about you.

You see, it's true; everything on the internet lasts.

Unlike now, we weren't taught to be as privacy-minded. Governments and corporations are fighting to wave privacy off as a paranoid's fantasy.

Many privacy groups exist and claim to fight for your rights against the invasion of privacy. But how many actually do help? Many are in bed with corporations and/or the government. Many just demand donations because of a believed slight. Others... others just steal content from each other.

The Paranoid's Bible?

We just want to spread knowledge.

We believe your various accounts should be like any good camp fire: Well planned.

You need to not only think it out but, also plan it out and have an emergency plan in case is spreads too far, too fast. Plus it doesn't hurt to have a plan to extinguish it.

Your online profiles and accounts shouldn't just rot. They need to be removed and all traces proving its existence also doused out. Like any good Woodsman or woman will tell you: A single campfire can destroy a forest.

This is why you must always plan your accounts and profiles out. Like a campfire left alone in a forest, a single account or profile can destroy an entire life.

Any one account and/or profile can decimate an entire person's image.

Yes, in theory, everything will remain cached, copied or saved on some server till the end of days.

And you may think that just deleting an account will wipe all traces of it, but that isn't the truth. Everything, even after deleting an account, is still there. By law, most sites and services have to keep everything on their servers for a few months to a year or more. So, in a sense, you can never delete an account, hence us saying you need to think.

There are services for doing background checks on everyone and everything for any reasons.

You have an online footprint and anyone can find it, there's nothing else to say.

You have a digital trail dedicated to all your old fanfics, photos or images and online debates.

There are steps that you can take to prevent your online footprint from growing. But nothing short of doxing yourself (**[1]** self doxing) and learning just how much of your information is online can help.

One issue is how you interact with others online.

Another issue is how much information you post on the internet.

All we can do is give you some simple suggestions before providing you the tools needed to self-dox.

Once done, save this information somewhere on your computer or a USB where other's won't find it. Hold onto this until you've read the rest of this guide. This information will help you delete and opt-out of as much as possible.

- Self doxing isn't the act of doxing oneself and posting dox for all to see. It's the opposite. It's the act of using the tools, tactics and knowledge often used in doxing to "meta-dox" oneself. This act's done in private, not in the public's eye. You're to find and delete any traces or information that's found through the "self-dox". This is to prevent possible doxing in the future. (E.G: Opting out and having your information deleted from Spokeo. Or deleting an old account you've associated with your real name).

Resources: Note, the below resources apply to all "Digital Footprint" chapters
Dox, doxing and how to prevent it.
How to prevent dox.
Maxx's anti dox handbook.
How to keep your personal information private.
How criminals use Google maps to case the joint.
How to delete things from the internet.
Don't get doxed in 5 steps.
How doxing works.
So you wanna learn how to prevent doxing?
School of Privacy – What is self doxing?

Find your Digital Footprint - Dossier:

The reason to why we're opting to use a dossier is because it'll allow you to sort the information that you find on yourself. It's an easy-to-use format, too. This serves as your go-to document, which I recommend that you save in a .txt.

We know many will not believe this to be useful. Many will say you can't stop the government or corporations from spying. But corporations or government aren't out to ruin your life or financial security. The people you have to worry about getting a hold of this information are civilians. They'll contact employers, family and friends all under the guise of social justice. With the right combination of information, they can guess passwords and security questions. They can even discover information you don't have on the internet with the proper combo.

The below contains some simplified descriptions of why each piece of information is useful.

Name: Even if common, a person's name (first and/or last) can help verify information. It can lead to more private information found through Google and other services.

Age: Like their name, their age can confirm certain information.

Birth date: Used to verify age and name, plus other information.

Location: A general location, like a city or state, can help locate an address. It can confirm their identity on social networking sites and application sites (among others).

Phone number: Verify name and location

Home address: What else to say? The home address can usually turn up images and misc information through Google.

Possible relations: Mother, father, brother, sister, boyfriend, girlfriend, friends…ETC. This can confirm other pieces of information.

Usernames: Using the same username over and over again can create a trail. By leaving one and telling others where you're going, you can create a trail, too.

E-mail addresses: A key to tracking people down, the e-mail address leads to many things.

Accounts: Links to accounts found on various websites, used to keep a list of where you've been.

Websites: Most likely has information you don't realize. Information can be found through a "whois" search

Misc information: Miscellaneous pieces of information that may seem crucial or of interest. For example: Mac Address, IP address, IDs, SSN, birth certificates…ETC.

Possible accounts: Similar username or other items that makes you believe an account's related.

Images: Can verify accounts; find Exif data…ETC.

Make two dossiers.

One with the information you know and recall, then a second one with the information that you've found online through the use of this guide.

Keep the two separate once done.

Compare them only after you've read this guide fully.

Find your Digital Footprint—Resources

It's important to keep track of the information found through the use of the provided dossier. We suggest that you also keep track of how each piece of information was found, as well as what led you to that discovery. This way you'll be able to *provide us with more insight and knowledge on how to prevent information from leaking. You also will be able to help us figure out how to remove it.

Remember, though, it isn't who you are. It's who you used to be and what you've once said. This is what most people look for when they wish to dox someone. It's the key to ruining someone, no matter how liked they are online. Knowing what someone said or did in the past will help ruin their present self.

Now, before you start, put yourself into the shoes of a stranger. You should think back to previous scenarios or cases where you've heard of doxing. The reason I ask this is simple: To see just how varied doxing can be and just how unethical it can get at times.

Think of it like this: Someone you've argued with. Think of someone who wished nothing short of a pox upon your genitals or the death of your dog. This person has decided to track every piece of information possible on you that exist online.

This hatred is what usually drives people onward toward their goal of doxing. They need to find information on someone and put them in their place. Or it's because they believe it's their moral right to track down those who wander away from the hive mind.

Once you get into this frame of mind, don't think of the information you know, but search for what you don't. Search for items posted in the present and past. You must find this information and use it. Add it to your dossier. You'll get a glimpse of what others see when they comb through your blog and internet past.

Now, to make this simpler for you, we're going to end this part with a links and miscellaneous resources.

Username:

- http://www.namechk.com/
- http://www.knowem.com/
- http://www.namecheckr.com/
- http://www.checkusernames.com/

General:

- http://www.spokeo.com/
- http://www.pipl.com/
- http://www.wink.com/
- http://www.peekyou.com/
- http://www.yoname.com/
- https://www.linkedin.com/
- http://www.search.yahoo.com/
- http://www.google.com/
- http://www.bing.com/
- http://www.reddit.com/
- http://www.wink.com/
- http://www.aad.archives.gov/aad/series-list.jsp?cat=GS29
- http://www.numberway.com/uk/
- http://www.vinelink.com/vinelink/initMap.do
- http://www.jailbase.com/en/sources/fl-lcso/
- http://www.publicrecords.onlinesearches.com/
- http://www.www.abika.com/
- http://www.www.freeality.com/
- http://www.radaris.com/
- http://www.twoogel.com/
- http://www.advancedbackgroundchecks.com
- http://www.yellowpagesgoesgreen.org/
- http://www.Intelius.com/
- http://www.PublicRecordsNow.com
- http://www.Smartzip.com

Social Networks:

- http://www.twitter.com/
- http://www.facebook.com/
- http://www.deviantart.com
- http://www.xanga.com/
- http://www.tumblr.com/
- http://www.myspace.com/
- http://www.yasni.com/
- http://www.socialmention.com/
- http://www.whostalkin.com/
- http://www.linkedin.com/
- http://www.formspring.me/
- http://www.foursquare.com/
- http://www.about.me/
- http://www.profiles.google.com/
- http://www.blogger.com
- http://www.photobucket.com/
- http://www.quora.com/
- http://www.stumbleupon.com/
- http://www.reddit.com
- http://www.digg.com
- http://www.plixi.com
- http://www.pulse.yahoo.com/
- http://www.flickr.com/

Location:

- http://www.whitepages.com/person
- http://www.maps.google.com/
- http://www.411.com/
- http://www.192.com/
- http://www.zabasearch.com/
- http://www.zillow.com

People:

- http://www.123people.com/
- http://www.peekyou.com/
- http://www.peoplejar.com/
- http://www.anywho.com/whitepages
- http://www.yahoo.intelius.com/
- http://www.findermind.com/free-people-search-engines/
- http://www.ipeople.com
- http://www.facebook.com/directory/people/
- http://www.skipease.com/
- http://www.zabasearch.com/
- http://www.wink.com/
- http://www.dobsearch.com/
- http://www.searchbug.com/
- http://www.nationwidecrafts.com/
- http://www.everyone411.com/
- http://wwww.Acxiom.com/
- http://wwww.MyLife.com/
- http://www.Zabasearch.com
- http://www.ussearch.com/
- http://www.peoplesmart.com/
- http://www.usa-people-search.com/
- http://www.spoke.com/
- http://www.SOBSearch.com/
- http://www.beenverified.com/
- http://www.peoplefinder.com/

Phone numbers:

- http://www.whitepages.com/reverse-lookup
- http://www.freecellphonedirectorylookup.com/
- http://www.fonefinder.net/

Images:

- http://www.tineye.com/
- http://www.saucenao.com/
- http://www.photobucket.com/
- http://www.revimg.net/
- http://www.iqdb.org/

Programs:

- Skype

Add-ons (for Firefox)

- Exif viewer

Whois:

- http://www.networksolutions.com/whois/index.jsp

Caches:

- http://www.archive.is (Can be used to make your own caches of pages)
- http://www.archive.org/web/ 0

You may have come across similar links from such sites as insurgen.cc. Or maybe from an image board with an /i/nvasion or /i/nsurgency board. You could've even seen it on some social justice blogger's anti-bigotry how-to. But these links...? They're actually well known and have been the staple of a lot of lists and guides on how track a person or persons down.

These links will help you find your own information and thus help you dox yourself.

Please remember: This is but a sampling. If you wish to see a larger chunk of the iceberg that invades our privacy then look at the supplementary guides.

Please hold off on the "opt-outs" until you've read this whole guide. We've organized the opt-outs to help you speed along with the removal of your information. We ask you to wait as we also have various tips and tricks to ensure you do it right.

- Searching a person a specific way leads to different websites that cache their information.

Resources:
Tools for opting out from data brokers
Giant list of data brokers
Data miners
Data brokers
Online information brokers
Info brokers
Giant list of data brokers to opt out of
How to take back your privacy from data brokers
SilverSteamPunk's Tumblr post

Find your Digital Footprint – Tactic

When one looks for information online, there isn't just a single way to go about it. It's a mess of tactics, resources, and Googling until one's fingers are raw from typing. Because of this, we've created a series of simple tactics for you to track down your information online. We also wish to show you how to counteract these tactics.

We're going to start with a simple tactic and lead onwards from there.

Applies to Tumblr only

- **About me leads to about you:**

Simple and fast, always the first thing you should do.

Look at the about me, see what information is there?

A name?

An age?

What about nicknames, or links, or a list of tags or posts…?

Whatever there is, it leads to valuable information that can pad out the dossier.

Counteract: Never use your real name online, nicknames, or anything of value. This should apply to any and all accounts you own.

- **Tumblr cataloging:**

This is simple, in all actuality, as it only requires time and patience, and lots of reading.

To start out, one goes to the target blog. Then you comb through the /archive/ link or by finding the last page of a blog. In theory, you need to find the oldest/first post made on the blog.

From there, working your way up to most current, you go from page-to-page. You skim posts for key pieces of information that can be used to find information elsewhere or used in any Search Engine.

Things you'll look for:

- Exif data from images
- Linked image albums
- Alternate blog or account links
- E-mail addresses
- Wish lists
- Personal rants
- Family or pet names
- Real life locations or school names

The older the blog, the more likely there are pieces of information used to find their accounts elsewhere online.

Counteract: Simply put—don't be ignorant or rash. Think, watch what you post, don't leak real world information, save images as PNG and always scrub the Exif data.

Be careful and post smart.

- **Tag hunt:**

The trend of having to tag every post caused people to be obsessive with certain tags.

To profit from this, one has to check for a "Tag list," or commonly used tags like "My face" or "Me". Depending on whether Tumblr pulled an Imgur and removes Exif data, images can lead to real world information. Certain tags can end up leading to accounts and personal information. These can accounts are found through simple reverse image searches.

Counteract: Post smart, save images as PNG and always scrub Exif data. Be general and misleading about thing in reality (when discussing online). Swap real names for generic names or handles—High school is now your High school, not Mt. Rush High.

- **Tag search:**

Search the blog's username and/or title on Tumblr search and Tumblr's tag search. You can also search previous or past usernames/titles.

You can find a lot out on a blogger and who they hang out with by searching them on Tumblr. If they have a previous blog name/title, it can be found by using the "Tumblr cataloging" tactic.

Example:

1. Party H re-blogged and responded to Party B.
2. The post Party B re-blogged was from Party A. The post from Party A is on Party H's blog.
3. Party H is the "Source," but older posts show it re-blogged from Party A.
4. This means Party H and Party A was one in the same and Party H changed the name/title.

Searching their previous names/titles on Tumblr can and will usually lead to excellent information. Remember though, you'll need patience and to take some time going through these tags.

Counteract: Don't change your title/name, or do so often.

- **Statcounter surfing:**

Use a publicly displayed counter or your own to track someone's IP down and blog(s).

To do this: Check for a Statcounter or tracker made public, or use your own and bait the target. Now look at what information is displayed and/or look for /blog/username links. Use these to find meta data like:

- Blogs
- IP address
- General location (ISP or host's location)
- Referral information

Counteract: Many add-ons help prevent this, like Umatrix or Ublock Origin. Always use one or more of these add-ons.

You've done all that you've could on Tumblr; you've gotten some information… now what?

Well, it's time to breakout Google or some other search engine. Now start using various combinations of the information that you've found.

General information and searching

- **Username searching:**

Search the Username using a search engine or one of several username check websites.

Just find any and all accounts with a similar username. You then check its information against that in the dossier.

Counteract: Never use the same username twice. Always change it, no matter what. Never share your accounts with anyone or announce your accounts elsewhere. Never inter-link accounts.

- **E-mail address surfing:**

Using any number of websites or search engines, one can enter an email address to lookup. Using its variations (@gmail, hotmail, yahoo…ETC) you can find miscellaneous accounts. This can also lead to information and possible dead-accounts or addresses.

You could use an address and resurrect it anew to claim accounts to learn information like passwords.

Counteract: Use a different E-mail address for each account. Having a "Main" that acts as the secondary account for the others one. Don't display your E-mail. Never give it out, or at least use a secondary-secondary as a fake for public display.

- **Account hopping:**

The older an account, the more likely it will link to another account somewhere else.

Like a few of the Tumblr tactics, one just has to search tags, keywords, and comb through the accounts. Usually it's a comment or even a keyword itself. Better success on Wordpress or Blogger accounts, also in descriptions on profiles.

Counteract: Always wait a month before deleting an account. Remove any and all posts, texts, and information. Before deleting the text or posts, first fill them with random characters/text. This is to force a new cache from various search engine and services. This should render previous ones inaccessible and only leave traces of nothing.

Example: Instead of a lengthy diatribe against your old SO, it's sldknlskndlfkndlkslfksldkfndslksdnflkskInfdslkfsdnklds). Also, for images or videos, upload blank images or static filled videos.

❖ **Photobucket jumping:**

Just searching usernames against account links like 'photobucket.com/user/-username-' or 'photobucket.com/profile/-username-' to find an account.

Once an account is discovered, people can search parts or the whole URL of any direct image link. This allows people to find where you've posted your images and thus your accounts.

Counteract: Delete your images and photobucket account. Don't put a password on it and don't let it idle…it'll lasts forever.

❖ **CTRL + U sourcing it:**

Check custom layouts on various blogging platforms for websites and links.

Various sites allow individuals to add their own custom flair to things. For example a layout and separate page designs. You can find links to storage accounts or image upload services by checking the source. This usually leads to photobucket accounts, imageshack accounts or personal servers. It could also expose a cloud storage account that can be searched or forced into exposing more information.

Counteract: Use the month rule and random text/character trick before deletion. You should also name all images randomly instead of using actual words. Don't put anything in obvious order.

Note on passwords: 8 to 12 characters long with random letters, numbers and characters.

❖ **Forum scouting:**

Found an account on a forum; search the forum for more information.

Most forums have a search function that allows you to search a username plus keywords. It's simple and quick.

Search specific things like:

- Social network names
- Usernames
- E-mails
- General keywords (example: email, account, art, location, school)

Double check posts for signatures or avatars that can be traced back to other accounts.

If that isn't possible, then check the user's profile for a post counter that may or may not be clickable. This will usually lead to all their posts.

Counteract: One month wait before delete plus random characters. Also request the owner/mods/staff to delete account and all posts.

- **Gaia Whoring:**

Go to their forums and search them, or profiles for similar usernames and information. Check against a search engine with things like “Username,” “Gaia,” “E-mail” and whatever else.

This usually leads to various forums and other accounts.

This tactic can also be applied to Neopets, among other sites.

Counteract: Follow the deletion trick of random characters…Etc. Don’t giveaway your items. Don’t donate your gold or cash. Just delete everything within the month rule.

- **Face snipping:**

Find a picture of someone online. Crop out everything but their face. Using the (cropped) image of just their face and/or head, go to Tineye and see if you can find results. Usually you’ll be able to find accounts. You can find account belonging to friends and relatives. You may also find a school websites or similar item where your target is photographed.

Counteract: Never post your image online, ever. Also scrub exif data.

These tactics are but a sampling of what many people do on a daily basis to find the information of others. We just list the most common and easiest to do for you to help you find your online footprint.

Find your Digital Foot print--Things you should know and do

This chapter is dedicated to providing you with various steps that you can take to prevent cross-referencing through multiple accounts. A single piece of information posted in one location can be used against you and lead to another account. If not taken into careful consideration, something as simple as your first name could lead to your inevitable doxing.

Imagine, if you will, that you have an account on a site about model trains. You signed up with your first name and used your old AOL e-mail address. Someone looking for you discovers you like trains; however all they have on you is an old username. They search this username, which is used in your old AOL e-mail address. They discover your model train account and first name. Search with various variations of your e-mail address and name, they discover a newsletter of your town's local hobby shop and model train group.

They now know your full name, your hobby group, your old e-mail address and several other pieces of information that, when combined, lead to your home address.

Congratulations, you've been doxed.

When leaving an account:

- When leaving, don't announce it.
- Tell no one that you're deleting your account.
- Delete your account only after a month of inactivity. And delete it only after switching it to a *'Dead E-mail address'.
- **Note:** An e-mail address used to take ownership of an account that you're deleting/deactivating.

Steps to take before deleting an account:

- Before deleting anything, wait a month.
- Anything you can edit, do so with random characters and text.
- Image should be replaced with a blank temp image (pure color image).
- Once a month is over, you can delete that account.
- But before doing so, delete the account's items one by one.
- If you can't delete something, ask the staff/owner/webmaster/mods to delete it for you.
- Stating that someone is stalking you is usually enough to remove the information.
- If they won't remove, try to edit it once again with random text.
- If you can't edit it, ignore it.
- If it's a blog, change titles and/or usernames.
- Preserve the original URL or username on a blank blog.
- Never leave your old username or URL up for grabs.

On removing an old E-mail address:

- Never delete an e-mail address, simply switch accounts and other items accordingly.
- Mark everything else in it as spam, but only if you can't unsubscribe.
- Log into it at least once a month to prevent deletion.
- You can, most likely, delete it, after not using it, around a year or two later.
- Always make sure the e-mail is no longer tied to any accounts or personal information.
- Always wipe it out like any other account by changing as much as possible to randomized text.

On account maintenance:

- Never use your real name.
- Never upload an image of yourself.
- Never use your real location.
- Never discuss your time zone.
- Never discuss your current time.
- Always use English, at all times.
- Never discuss events happening in your area.
- Never mention race or skin color.
- Never mention religion.
- Never mention sexuality.
- Never discuss your hobbies in great detail.
- Don't talk about your fetishes or kinks.
- Accounts shouldn't be cross-linked through various accounts/sites.
- If you do, make sure no username is the same.
- And make sure no e-mail address displayed is the same.
- Use a different e-mail address for each account.
- Keep accounts separate if not needed to be linked.
- Never link RP accounts to other accounts and social networking profiles
- Don't mention how many pets you have or their names.
- The same applies to family members, neighbors, friends, and significant others.
- Scrape as much information off of something as possible.
- Boil it all down to the core basics.
- Never keep an account longer than a year (some exceptions apply).

On talking to strangers:

- Never display your messenger, Skype or chat names anywhere online.
- Give it to others only if they ask you.
- Keep all forms of instant messaging and chat private.
- Don't save logs.
- Only give out to trusted individuals.
- This applies to IRC channels and chat setups.
- Lock down as much as possible.
- Never use real names or information, ever.
- Don't tell other people who you talk to online.
- Never place your full name on Skype.
- Limit the profile you have on Skype.
- Make sure all Skype options are set to private.
- If it can't be set to private, then set to contacts.
- Like Skype, any chat client or instant messenger should be locked down.

On behavior:

- You'll most likely have to change the way you behave online.
- Sharing interests is fine, but getting too obsessed is bad.
- Never admit to liking any specific thing
- This can help people tie other accounts to you.
- Admitting to things, like, your favorite food can be used to trace too.
- In general, you need to keep yourself and your information limited when on the Internet.
- Instead of admitting to liking a song, just say you like the band.
- This applies specific bands in a genre.
- Or any form of entertainment that you specifically like.
- Instead of specific parts you like in a game, you just like the game.
- Remember: don't talk about your location.
- Don't talk about your general location in detail.
- Don't mention what it's known for (produce, exports, colleges, universities...etc).
- Don't make mention of recent weather, as that can be used in junction with other information
- Don't say the exact time.
- Be wary of saying exactly what the temperature is.
- If the person you're talking to uses Celsius, then tell the temp in Celsius.
- If the person you're talking to uses Fahrenheit, then tell the temp in Fahrenheit.
- Don't make mention of general information like school names or street names.
- Don't make mention eateries/restaurants as they can be unique to your location only.
- Always refer to your city/town as a college town.
- Never post selfies.
- Never post nudes.
- Never post porn.
- Never post erotica.

When getting personal:

- Don't discuss siblings or family members to great extent.
- Don't drop pet names.
- Don't drop the name of anyone related to you.
- Don't drop the name of friends.
- Don't drop the name of politicians.
- Don't drop the names of people you've had relationships with.
- Keep age to a general rounded number, like, the 20s…etc
- Keep personal descriptions down.
- Keep weight to a more general descriptor (overweight, obese…etc).

On talking about life experiences:

- Never do so in the first place.
- If you do, don't let incriminating evidence be traced back to you.
- Or at least make sure you can discuss such things in a secure environment.
- Also don't attach anything about you to your online personas and/or accounts.

On using custom domains:

- Ask your host about Whois masking.
- If they don't offer it, check into other services.

On online relationships:

- Don't do online dating.
- Don't sext.
- Don't cyber.
- Don't do erotic roleplay.
- Don't go to online dating websites.
- Don't take part in relationship, dating, sex…etc help sites/forums/chats.

Just use common sense.

The Paranoid's Rules

The below is a mix of "common sense" rules that don't have any real place in the above chapters, yet have proven to be somewhat useful.

1. Don't ever use your real name online
2. DO NOT EVER POST YOUR REAL NAME ONLINE
3. Never use the same username, ever, anywhere online
4. Never interlink or make mention of your accounts anywhere online
5. Always use a different e-mail for each account, never mention them online
6. Always use a 10 to 15 character length password
7. Always use a mix of random characters
8. Always change your passwords, if you've logged in recently, at least weekly
9. Never post your IRL location online (state, city…etc)
10. Never post your IRL address online
11. Never give out your phone number, ever
12. Never give out your cell phone number, ever
13. Never post your photos online, ever
14. If you break #13, at least scrub as much Meta-data as possible from your images
15. Never post anything that you, yourself, haven't gotten over
16. If data exists, you are at risk
17. Anonymity is your greatest offense, defense, weapon and friend--don't lose it
18. Never post your e-mail addresses anywhere online
19. You are nothing more than another random user online. Disregard everything that makes you an individual.
20. Choose your battles carefully. There may not be many geniuses out there, but there are plenty of smart idiots.
21. Avoid Social Networks and media
22. If you break #21, remember the previous 20 rules
23. Don't sexualize the Miku
24. Disregard #23; never sexualize anything, ever, you perverts
25. Getting involved in anything pornographic or erotic will lead to your doxing, eventually
26. E-drama isn't drama; it's a temporary temper tantrum
27. Disregard E-celebs, get a personality
28. Don't drink and surf, or blog, or post, or anything, ever
29. /b/ may be the asshole of the Internet, but Tumblr is the cancer of everything good in the world
30. Doxing and Tumblr go hand in hand, avoid Tumblr
31. Internet dating is a scam, go buy something from Bad Dragon
32. Seriously, don't E-date, you nerd
33. A fetish is a disorder, and the word misused
34. @#33, a kink is what you have, not a fetish
35. @#34, preferences can be both kinks and/or a fetish
36. @#35, if you can't get off without something specific or it interferes with your life—it's a fetish
37. @#36, if you have trouble telling the difference between a fetish, a kink, or a preference—seek professional help
38. Children are smart idiots; don't let children have their own computers
39. If you ignore rule #38, don't let them have an active Internet connection

40. In regards to #39, don't let them have a device with WiFi capabilities
41. Never share an account, ever, with anyone
42. Always logout of an account, if you get up for any extended period of time
43. ALWAYS LOGOUT OF YOUR ACCOUNTS, EVEN IF YOU AREN'T ON A SHARED COMPUTER
44. SERIOUSLY, ALWAYS LOGOUT OF YOUR ACCOUNTS, ESPECIALLY ON A SHARED COMPUTER
45. NEVER LOG INTO AN ACCOUNT IF THE DEVICE YOU'RE USING ISN'T YOURS
46. Don't bank online, or use your cell phone, or a borrowed device—bank IRL
47. It's FREEDOM OF SPEECH not FREEDOM OF HARASSMENT—you can use FoS to call out harassment and stupidity, though
48. If you feel threatened, harassed, or don't want contact—TELL THEM TO LEAVE YOU ALONE
49. @#48, learn to use the block tools and learn to never put trust in anyone or an account
50. @#49, sometimes it's best to pick up and move to another account to avoid trouble and harassment
51. @#50, it's the Internet… turn it off and you end trolling and e-bullying
52. Harassment has to mean they threatened you or you told them to leave you alone. It doesn't mean you felt uncomfortable because of them saying or doing something
53. @#51, learn to move on and ignore, if not: You deserved it
54. The Government may not be your friend, but an individual can
55. @#54, don't be rude to police, doctors, nurses, military personnel, politicians or anyone, ever
56. @#55, unless they did something illegal or dangerous, then remain on the fence and review all the facts.
57. @#56, always make an educated and well researched decision. Never trust a single source. Sources that contradict or are against each other provide a lot of insight and information one or the other didn't show
58. Men and Women are corruptible, as are you. Learn what you say and do affects others too, besides yourself
59. Most political movements or (sic) groups aren't about freedom or (sic)'s agency. Many are for the subjugation of society in the name of equal outcome. Even if it means shared adversity and ignorance
60. They may be men or women of the badge, cloth or science but they are still men and woman
61. Trust but verify
62. Don't just listen and believe
63. Intelligence doesn't equate wisdom
64. And wisdom doesn't equate intelligence
65. An education doesn't guarantee experience or knowledge
66. A degree and/or diploma is just a piece of paper
67. Everyone does something for a reason, even if they're unaware of it
68. @#67, there are no Jokers or Banes
69. @#68, the world burning is hardly ever funny to a man who proclaims it to be
70. Always unplug your modem and/or router
71. @#70, always do so when not in use
72. @#71, or when you plan to turn off your computer
73. @#72, just unplug it if you don't actively need it
74. WiFi is bad, don't use wireless Internet
75. @#74, if you do, don't log into anything important lest you risk getting your accounts being hijacked
76. It's the Internet, not a social meet and greet, stop seeking attention.
77. If you claim to be anything but human on the Internet, expect to be harassed, rightfully so

78. You lie to the Internet and it'll learn the truth sooner than later
79. The Internet is compromised of mostly normal people who wish to appear to be quirky or unique
80. If you've time to complain about your physical appearance or lack thereof… you've time to improve yourself
81. Everything is opened to critique if posted online
82. @#81, but learn to critique is to open yourself up to criticism
83. @#82, but to critique someone for critiquing shouldn't be used as an excuse to silence criticism
84. @#83, though it is better to be a creator than a user
85. @#83, but it doesn't mean that a user's criticism isn't valid
86. @#85, sometimes the customer sees and tastes things the chef does not
87. A username adds weight to your opinions
88. @#87, being anonymous does not
89. @#88, but having a username makes you easier to attack and destroy
90. AVOID USING CAPS ALL THE TIME
91. @#90, basic grammar, spelling and punctuation are your best bet
92. @#91, but avoid using overly complicated words
93. @#92, and avoid being wordy
94. @#93, and avoid using memes, slang or shortened words or phrases
95. Memes are inside jokes exploited and taken from one source and posted to another source
96. @#95, avoid using memes
97. @#96, avoid memes at all cost
98. Simple, blunt and to the point when trying to relay any thought is usually better than a long winded and wordy rant
99. It's the Internet, not school
100. @#99, It doesn't mean be an imbecile and forgo all common sense for acceptance
101. Don't click on unfamiliar links
102. @#101, avoid shortened links
103. @#102, avoid links hidden behind a link shortener service
104. @#103, don't click on links from strangers
105. @#104, avoid links from people you don't trust
106. @#105, avoid links in general unless you know exactly what you're clicking on

Opt-out Master-list

The purpose of this chapter is to provide you with an up-to-date listing of any and all opt-outs. This means you'll be able to opt-out of not only known data brokers but several unknown brokers. You'll even cut down on physical mail and e-mail.

Many feel this isn't needed as you have to provide information to remove information, but this is what's needed. Not just by the law but also for business records. Opt-outs are just you acknowledging a contract made without your knowledge.

Instead of ignoring them, you're stating you don't want them using or selling your information. It not only helps reduce your online footprint but also helps you cut back on carbon emissions. You also cut back on your exposure online.

For now, we've only include the online opt-outs in this PDF. We suggest you finish those and those alone as most of them are interlinked to many of the phone and fax opt-outs. Once you finished those you should wait a month or two before doing other opt-outs. A lot of information will be expunged as you opted out of one or two other sites.

Online Opt-outs:

These are opt-outs that can be done online through forms or simple links without a pay wall.

http://www.10digits.us/
http://www.10digits.us/remove
Requires photo ID upload + e-maill addess + page link
Make sure to search using all three methods
Repeat for each immediate family member in your residence

http://www.411.info
http://www.411.info/contact/
Find your info, copy the link.
Go to the contact link and ask them to remove your info.
Provide the link(s) in the message.

http://www.500millionphonerecords.com/
http://www.phonedetective.com/PD.aspx?_act=OptOut
Follow the instructions on the Phonedetective opt-out link.
Repeat for each individual in household and any and all numbers you've owned or recall owning

http://www.accutellus.com/
http://www.accutellus.com/opt_out_request.php

Follow the instructions on the opt-out page, repeat for all individual in household

http://www.Acxiom.com/
http://www.isapps.acxiom.com/optout/optout.aspx
(Cookie opt-out can be ignored if you install ad blocking and privacy based add-ons on your rig)
For the actual opt-out, just follow the above link and follow the instructions, repeating it for each residence in your house.
After each successful entry fill out, you'll be taken to a new page with a capatcha and a field to confirm the e-mail address
Log into your e-mail account, find the confirmation e-mail, and follow the link provided
Repeat for each individual in household

http://www.addresses.com/
http://www.addresses.com/optout.php
Follow instructions on page, repeat for each individual in household

http://www.addresssearch.com/
http://www.addresssearch.com/remove-info.php
Follow instructions on page, repeat for each individual in household

http://www.allareacodes.com/
http://www.allareacodes.com/remove_name.htm
Follow instructions on page, repeat for each individual in household

http://www.archives.com/
http://www.archives.com/ga.aspx?_act=Optout
Follow instructions on page, repeat for each individual in household

http://www.checkpeople.com/
http://www.checkpeople.com/optout
Follow instructions on page, repeat for each individual in household

http://www.corporationwiki.com/
http://www.corporationwiki.com/profiles/public
Follow instructions listed on their website.
Very few cases, only for businesses and their executives.

http://www.coxtarget.com/
http://www.coxtarget.com/mailsuppression/s/DisplayMailSuppressionForm
Wait until you've received your next "ValPak" packet\envelope
Go to Opt-out form\link above
Enter information as it is on the envelope
You've opted out

http://www.datalogix.com/
http://www.datalogix.com/privacy/#opt-out-landing

http://www.aboutads.info/ (More info here)
Find this sentence "If you wish to opt out of all Datalogix-enabled advertising across channels including direct mail, online, mobile and analytic products, and click here."
Follow directions, repeat for each resident of household

http://www.dexone.com/
http://www.dexknows.com/
http://www.dexpages.com/index.asp?
http://www.dexone.com/privacy-policy
http://green.dexknows.com/DexGreen/selectDexAction.do
Enter zip code
Follow directions
If you can't opt-out, you can do so VIA the Yellow Pages opt-out

http://www.directmail.com/
http://www.directmail.com/directory/mail_preference/
Follow directions in second link

http://www.dmachoice.org/
http://www.dmachoice.org/register.php
Follow directions on website
Have to create an account for each member of household

http://www.dobsearch.com/
Search yourself, address, phone number…etc
Find info
Look for "Is this you? Manage your listing!"
Follow instructions (You'll need a valid e-mail address + landline or cell)
Repeat for all residences in house (One per 24 hours)

http://www.donotcall.gov
http://www.donotcall.gov/register/reg.aspx
Follow directions
Enter phone numbers, cell and/or landline, and an e-mail address

http://www.ebureau.com/
http://www.ebureau.com/privacy-center/opt-out
Same as DMA choice opt-out, but no accounts; you'll have to do this with previous addresses too

http://www.emailfinder.com/
http://www.emailfinder.com/EFC.aspx?_act=Optout
Follow instructions on screen
Repeat for each resident in household

http://www.epsilon.com/
http://www.epsilon.com/consumer-preference-center

http://www.optoutprescreen.com
Go to third link and follow their process (only need to be done once)

http://www.everify.com
http://www.everify.com/legal.php#2
http://www.everify.com/legal.php#remove
Follow instructions on page, repeat for each individual in household

http://www.experian.com/
http://www.experian.com/privacy/opting_out_preapproved_offers.html
http://www.optoutprescreen.com
Go to third link and follow their process (only need to be done once)

http://equifax.com/
http://help.equifax.com/app/answers/detail/a_id/2/noIntercept/1/kw/prescreen
http://www.optoutprescreen.com
Go to third link and follow their process (only need to be done once)

http://www.everyone411.com/
Go to contact page @ http://www.everyone411.com/contact
Provide listing links
Request removal
Repeat for all individuals in household

http://www.freephonetracer.com/
http://www.freephonetracer.com/FCPT.aspx?_act=OptOut
Online opt-out form, follow directions.

http://www.health.com/health/
http://subscription.timeinc.com/storefront/privacy/health/generic_privacy_form_offline.html?dnp-source=E%20AND%20
http://subscription.timeinc.com/storefront/privacy/health/generic_privacy_form_online.html?dnp-source=E
Fill out with your information, repeat for each individual in your household. Make sure to check all boxes in the two opt-out links.

http://www.ims-dm.com/
http://www.ims-dm.com/cgi/optoutemps.php
Follow directions on second link
Enter up to three emails
Fill captcha
Clear cache and repeat as necessary

http://www.infousa.com/
http://www.infousa.com/StaticPage/PrivacyPolicyInfo.htm

Look for: Opt Out Policy–Upon a visitor's request, InfoUSA Inc
Read it carefully, scroll down and find the "E-mail form"
Fill it out, include your name, birth date, address and phone number. Request all information of yours to be removed, especially anything related to the info you just provided.

http://www.infospace.com/
http://www.support.infospace.com/privacy/
Search for "Choice/Opt-out"
The link there is old, use this one: http://infospace.com/contact/index.html
Select "General inquiry"
Provide your name, birth date, address and phone number
Request all information of yours be removed, especially anything matching or related to information you just provided

http://www.innovis.com/
http://www.innovis.com/InnovisWeb/pers_lc_opt_out.html
www.optoutprescreen.com
Go to third link and follow their process (only need to be done once)

http://www.instantpeoplefinder.com/
http://www.instantpeoplefinder.com/optout.php
Follow on page instructions, repeat for each individual in household

http://www.locatefamily.com/
http://www.locatefamily.com/contact.html
Search for your name on the Left side of the site
You'll find a page or pages containing Names, addresses and phone numbers
Find yours; take note of the number next to it
Go to the contact page
Scroll down for the opt-out\removal form
Follow the directions
Make sure to provide the information you want deleted in the "Comments" box
Repeat for each individual in household

http://www.lookup.com/
http://www.lookup.com/optout.php
Go to the opt-out link
Follow the directions
Repeat for each individual in household

http://lycos.com
http://info.lycos.com/resources/privacy-policy
Search for: How can you access or edit your information?
Follow directions

http://www.mobilephoneno.com/
http://www.mobilephoneno.com/help.htm

Search for “How do I delete my entry?”
Follow directions

http://www.militaryavenue.com/
http://www.militaryavenue.com/Contact.aspx
Businesses only
But, if you have your information up there, somehow
First find said info
Go to the contact page
Select, from the drop down, “Incorrect Business information”
Provide link, info, and ask for removal

http://www.myyp.com/
http://www.yellowpagesoptout.com
Follow instructions on second link

http://www.nationwidecrafts.com/
Find listing
Click the suggestion link/light bulb icon
Request removal

http://www.orientaltrading.com/
http://www.orientaltrading.com/ui/help/processRequest.do?requestURI=link.removeForm
Follow instructions on second link

http://www.peekyou.com/
http://www.peekyou.com/about/contact/optout
Search for yourself
Locate your profile and right-click then select 'copy link'
Then open a new tab and go to their opt out page and follow the instructions provided.
Repeat with each individual in household

http://www.peepdb.com/
Enter full name + state
Look for city + state in results
Can confirm by partial phone # listed
Click your result
Scroll down
Click “Remove This Listing”
Follow directions
Takes 10 business days
One request + IP every 3 days
Repeat with each individual in household

http://www.peoplebook.com/
http://www.peoplebook.com/support.htm

Search for your people book's results
Confirm it's yours
Grab link
Go to the support link
Follow directions
Repeat for each individual in house

http://www.peoplefinder.com/
http://www.peoplefinder.com/manage/
http://www.peoplefinder.com/optout.php
Go directly to the opt out link
Fill in your information
Select from the drop down "General privacy concerns"
Enter the code word and click submit
Repeat for each individual in household

http://www.peoplefinders.com/
http://www.peoplefinders.com/manage/default.aspx
Search your first, middle and last name in search
State + city, too
Find your listing, click "this is me"
Skip the AD and\or sale section
Takes anywhere from an hour to a month
Repeat for each individual in household

http://www.peoplesearchpro.com/
http://www.peoplesmart.com/optout-go
Go directly to Opt-out
Enter your name + city and state
Find it, click it, and follow directions
You will have to make an account
Repeat for each individual in household

http://www.peoplesmart.com/
http://www.peoplesmart.com/opt-out?
Follow the People Smart opt-out instruction
You'll be shown a page of results, locate yours
Click the "This is me"
Look at the "Business" listings, find anything of yours and click the "This is me" or skip the step if none exist
Uncheck all options, except the last two
Click "Save Settings"
It'll have you create an account, make sure to use a unique password only for this site and use nowhere else
Repeat for each individual in your household (sans the account)
Repeat search, but this time with home address applied
http://www.peoplewise.com/
http://www.peoplewise.com/show/optoutdisclaimer

Go straight to the opt out link
Make sure JS and Cookies are enabled
Follow the steps; make sure to read the red text
When you find your list, click the “Removal” test under the blue button
When you’re on your page, within the red text, is a blue link, click it
Enter your email address + security code
Repeat for each individual in household

http://www.phonebook.com/
http://www.whitepages.com/privacy_central#6
Go to Whitepages.com
Create an account
Search for your information VIA address, name, phone number...etc
Claim each and every piece of information that's confirmed as yours
Verify through e-mail and phone
Then go to your profile
Scroll down and request your information to be hidden\removed from the directory
Follow the on screen prompts
Logout, clean cache
Create an account for each individual in household, repeat until finished

http://www.phonebooks.com/
Search your name + city and state
Find your listing in the results
Click on said listing
Locate “Remove this person”
Follow directions
Repeat for each and every individual in household

http://www.phonedetective.com/
http://www.phonedetective.com/PD.aspx?_act=OptOut
Go directly to opt-out page, follow directions
Repeat for each individual in house
Also repeat with each phone number you have or recall having

http://phonenumber.com/
http://www.whitepages.com/

http://www.whitepagescustomers.com
http://www.whitepagescustomers.com/draft-how-do-i-remove-my-people-search-listing/
Create an account
Search for your information VIA address, name, phone number...etc
Claim each and every piece of information that's confirmed as yours
Verify through e-mail and phone
Then go to your profile
Scroll down and request your information to be hidden/removed from the directory
Follow the on screen prompts
Logout, clean cache
Create an account for each individual in household, repeat until finished

http://www.poedit.org/
http://www.poedit.org/auth/removal_request.html
Search for your page/information
Take link/URL
Copy it to the appropriate area listed in the second link
Submit
Find confirmation e-mail in email address
Repeat for each individual in household

http://www.privateeye.com/
http://www.peoplefinders.com/manage/
Go to the People Finders link
Enter your information
On the results page you can refine your searches with age + birthdate
Find your results and click "This is me"
Follow instructions
Repeat for each individual in household

http://profileengine.com/
http://profileengine.com/#/help
http://profileengine.com/#/claimprofile
Search for profile
Look for the claim profile option
If not present, try the claim profile link above
Follow instructions
Repeat for each individual in household

http://pub360.com
http://pub360.com/s/faq
Search for your name
In results, look for the 'Information Removal' tab
Follow instructions provided
Repeat for each individual in household

http://radaris.com/
http://radaris.com/removal/

http://radaris.com/page/how-to-remove
Search for a name.
On the search results page, select the name that is most appropriate.
On the profile page, click the down-arrow to the right of the name and select "Control Information".
From the information control page, choose "Remove information".
Here you can choose to remove all information, or to delete specific records.
Confirm your real name matches your account and profile name.
Enter your cellular phone to receive a verification code.
Once the code has been entered, the profile will be private.
Repeat for each individual in household

http://www.redplum.com/
http://www.redplum.com/tools/redplum-postal-addremove.html
Follow the instructions provided on the second link
Per known address

http://www.reversephonelookup.com/
http://www.reversephonelookup.com/remove.php
Go to second link
Follow instruction provided
Repeat for all known and owned phone numbers

http://www.searchbug.com/
http://www.searchbug.com/help.aspx?WHAT=people
Search for your name + city and state
If “Free record” is shown, you can click the garbage can\remove link to have it removed
Repeat for all individuals in house
Note: Premium records can't be removed through this process as they require manual removal and cost payment to do so

http://www.Spokeo.com
http://www.spokeo.com/optout
Go to Spokeo
Search your First, middle and last name
Find your profile/listing by go to the bottom of the page and select "open advance filter"
Fill out your information
Find your profile/listing, copy the link (note: Right click+ copy link to have a "Clean link" copied)
Go to the Opt out link
Follow instructions to opt-out
Repeat for each individual in house
Hint: You’ll need a different e-mail address after so many removals
Hint: You may have multiple profiles\links due to previous addresses
Hint: Make sure HTTPs is not at the start of the link, if it is just remove the 'S'.

http://www.usa.com
http://www.peoplesmart.com/

http://www.peoplesmart.com/opt-out
Follow the People Smart opt-out instruction
You'll be shown a page of results, locate yours
Click the "This is me"
Look at the "Business" listings, find anything of yours and click the "This is me" or skip the step if none exist
Uncheck all options, except the last two
Click "Save Settings"
It'll have you create an account, make sure to use a unique password only for this site and use nowhere else
Repeat for each individual in your household (sans the account)
Repeat search, but this time with home address applied

http://www.usa-people-search.com/
http://www.usa-people-search.com/manage/default.aspx
Go to the "Manage" link
Enter your information
Find your listing
Enter Captcha and tick both boxes
Repeat for each individual in house

http://www.usbizplace.com/
http://www.usbizplace.com/contact-us.html
Find your listing with your information
Follow directions on the contact-us page
Repeat for all listings of yours you wish to remove

http://www.webcrawler.com/
http://www.webcrawler.com/support/privacypolicy
http://www.webcrawler.com/support/contactus
Go to Webcrawler.com, search for your info
Select link + note its order in the listing
Contact them at the 'Contact us' link
Request removal due to privacy concerns
Repeat for each individual in household

http://www.whitepages.com/
http://www.whitepagescustomers.com
http://www.whitepagescustomers.com/draft-how-do-i-remove-my-people-search-listing/
Create an account
Search for your information VIA address, name, phone number...etc
Claim each and every piece of information that's confirmed as yours
Verify through e-mail and phone
Then go to your profile
Scroll down and request your information to be hidden\removed from the directory
Follow the on screen prompts
Logout, clean cache
Create an account for each individual in household, repeat until finished

http://www.valassis.com/
http://www.valassis.com/1024/Contact/MailingListRemoval.aspx
Follow instructions on second link
Repeat for all known addresses

http://www.valpak.com/
http://www.coxtarget.com/mailsuppression/s/DisplayMailSuppressionForm
Wait till next envelope comes in the mail
Enter the info exactly as it is on the envelope
Repeat for all known addresses

http://www.wyty.com/
http://www.wyty.com/optout.aspx
Enter cell number (or phone number)
Select 'Request'
Should be removed within 24hrs to a month
Repeat for all known numbers

http://www.yellowbook.com/
https://www.yellowpagesoptout.com/
http://delivery.ypg.com/en/US/Home/Index/ (Canada opt-out)
Follow directions on 'Yellowpagesoptout' link
Enter zip\area code
Create account
Select items to opt-out
Repeat for all known addresses

http://www.yellowpages.com
http://www.yellowpagescom.intelius.com/optout.php
Fill out opt-out form
Repeat for each individual in household

http://www.yellowpagesgoesgreen.org/
http://www.yellowpagesgoesgreen.org/terms_of_service.php?#privacy
On the page with your information, look for “Are you the business owner”
Click it, select “Delete\remove listing”
Simply state your privacy concerns
Repeat for each individual in household

http://www.ziplocal.com/
http://ziplocal.com/online-privacy-policy/
http://www.ziplocalonline.com/manage-listings
To update your listing, use the search box above to look for your business.
When you locate your business, simply select the Update Business link and follow the instructions.

http://www.zoominfo.com/
http://www.zoominfo.com/lookupEmail
You'll be asked to provide your e-mail address
They'll search your address against their database
You'll receive an e-mail concerning whether or not they've your e-mail address
If not, nothing to worry about, but if they do they provide a means to opt-out.
Repeat for each individual in household

Miscellaneous Opt-outs:

This list contains opt-outs that have no direct place but have proven useful.

https://www.ameridex.com/
https://www.ameridex.com/privacy.html (review privacy policy for more info)
1. Another website that wants you to send an e-mail or send direct mail\snail mail opt-outs.
2. Also needs court order or proof of potential harm.

https://archive.org/
https://archive.org/about/exclude.php
https://web.archive.org/web/20140812200246/http://www2.sims.berkeley.edu/research/conferences/aps/removal-policy.html
1. If you're allowed to modify your account or website's HTML, add this somewhere in between the <head> tags
2. <META NAME="ia_archiver" CONTENT="NOINDEX, NOFOLLOW">

http://www.Bing.com
http://ssl.bing.com/profile/history?oma=toggle_off
1. Disable personalized nonsense and ads

Remove your property's street view on Bing Maps:
1. Go to: http://www.bing.com/maps/
2. Type home address
3. Get to street view
4. Center squarely on house
5. Look for (?) question mark near bottom right. Becareful as it can be hidden sometimes.
6. Click it
7. Select "Report an image concern"
8. You'll get a pop-up or new tab with a panoramic image
9. Select your house, a little red square will appear then
10. Voice your privacy concern, stating vandalism and potential break-ins by criminal elements who use online maps to scout\case potential targets
11. Fill out the rest of the form + Capatcha, wait
12. Save ticket (#) Number

http://www.catalogchoice.org/
1. Join site with an e-mail and password used nowhere else
2. Search for the catalogs you've received
3. Follow instructions to opt-out
4. This site just organizes websites; they aren't associated with any of them

http://courtclick.com/
http://courtclick.com/terms.php
http://www.courtclick.com/support/
1. Look for "Opt Out Policy: Note that public records such as court records can be updated or corrected, but not removed unless expunged, sealed, court ordered or the like."
2. You'll need to have your records sealed first.

http://www.emailtracer.com
http://www.emailtracer.com/tos.php
1. Search for "Opt Out Policy"
2. Only under certain circumstances

https://www.facebook.com/settings?tab=ads&view
1. Edit button in your Ads settings page, selecting No one and saving your changes.

http://www.Google.com
https://plus.google.com/settings/endorsements
http://www.google.com/ads/preferences/
https://history.google.com/history/
1. These links help make sure your Google data stays yours
2. You can opt-out of having your likes and such shared
3. Help limit ads and similar issues
4. And even help prevent your history on your account from being given out

Remove your property's street view on Google Maps:
1. Go to Google Maps and type in your address
2. Bring up the street view of your property
3. Look to the bottom right hand corner of the screen you should see an Icon Labeled: “report a problem.”
4. Click on “report a problem.”
5. You will get a page labeled “report inappropriate street view.”
6. Look for the words “Privacy Concerns” and click on them.
7. If you want your house blurred, click on “my house.” Then choose the option: “I have a picture of my house and would like it blurred.”
8. Adjust the image and show Google which part of the photo needs blurred.
9. Type the verification code at the bottom of the page into the box provided and click submit.
10. Check back in a few days to see if the image has been blurred.

http://www.lexisnexis.com/
http://www.lexisnexis.com/privacy/directmarketingopt-out.aspx
http://www.lexisnexis.com/privacy/for-consumers/opt-out-of-lexisnexis.aspx
1. requires you to have a court order or police report, but you can remove \some\ information through the Direct Marketing Opt-out, though.

http://www.locatepeople.org/
http://www.locatepeople.org/index.php?xpath=privacy
http://locatepeople.org/index.php?xpath=lp_optout
1. Can Opt-out only by certain circumstances

http://www.jailbase.com/
http://www.jailbase.com/en/opt-out/
1. Follow instructions on page, only under certain circumstances

http://www.justmugshots.com/
http://support.justmugshots.com/forums/21326676-Removal-Services
1. An odd one, but has shown some use

http://www.Publicrecordssearchonline.org
http://www.publicrecordssearchonline.org/new/faq.php
1. Search for "Q: How can I remove my information from the Public Records Database?"
2. Follow directions provided

http://twitter.com/settings/security
1. Through your profile, go to your Security Settings page and uncheck the box under the promoted content section.

http://www.Yahoo.com
http://www.info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html
http://www.search.yahoo.com/preferences/preferences?
1. Log into account
2. Disable ads and personalized stuff

http://www.Yahoo.com/maps

1. Visit http://www.Yahoo.com/maps
2. Drag the gray icon that resembles a person (top-right) to your street. (If it won't drag, then your street has not been photographed for Yahoo.)
3. Click on "report image" at the bottom-left of the screen. It will take you to a different website.
4. Click on "request blurring," and follow the directions.

http://west.thomson.com/
http://static.legalsolutions.thomsonreuters.com/static/pdf/opt_out_form.pdf
Only under special circumstances

What to do if doxed

This chapter is to help people learn how to react to not only being doxed but harassed through phone or mail.

Before we begin, I must note that we'll forego chapters and mini-sections. There isn't all that much to say or suggest that isn't covered by the other testaments and this PDF already. So think of this as nothing more than a simple refresher course or a go-to quick guide.

First:
If you're ever doxed, and you've never bothered keeping private, you need to learn not to react. Don't react, ever. Don't acknowledge it. Don't taunt. Don't say they have the wrong information.

DO NOT DO ANYTHING!

You let them know it's bothering you and the further they'll press to get a greater reaction out of you.

You just need to take things slow, and if it's a forum or website try reporting the post and account. But, remember, only do this after you've assessed the situation.

Also, remember: Even if the information is wrong, don't react. It could be an attempt at baiting you into providing your real information.

Second:
Blur out your house on Google, Bing and Yahoo maps.

The instructions are below:

For Bing:

1. http://www.bing.com/maps/
2. Type home address
3. Get to street view
4. Center squarely on house
5. Look for (?) question mark near bottom right. Be careful as it can be hidden sometimes.
6. Click it
7. Select "Report an image concern"
8. You'll get a pop-up or new tab with a panoramic image
9. Select your house, a little red square will appear then
10. Voice your privacy concern. Stating vandalism and potential break-ins by criminal elements.
11. Fill out the rest of the form + Capatcha, wait
12. Save ticket (#) Number

For Google:

1. Go to Google Maps and type in your address
2. Bring up the street view of your property
3. Look to the bottom right hand corner of the screen you should see an Icon Labeled: “report a problem.”
4. Click on “report a problem.”
5. You will get a page labeled “report inappropriate street view.”
6. Look for the words “Privacy Concerns” and click on them.
7. If you want your house blurred, click on “my house.” Then choose the option: “I have a picture of my house and would like it blurred.”
8. Adjust the image and show Google which part of the photo needs blurred.
9. Type the verification code at the bottom of the page into the box provided and click submit.
10. Check back in a few days to see if the image has been blurred.

For Yahoo: Special thanks to /r/n0esc from Reddit!

1. Visit http://www.Yahoo.com/maps
2. Drag the gray icon that resembles a person (top-right) to your street. (If it won’t drag, then your street has not been photographed for Yahoo.)
3. Click on “report image” at the bottom-left of the screen. It will take you to a different website.
4. Click on “request blurring,” and follow the directions.

Third:
Change your phones’ voice messages to the default robotic one. This is to prevent people from confirming and verifying your number as being related to you. This also hinders people and will push some off of harassing you.

Fourth:
Never answer the phone for anyone you don’t recognize. Names and phone numbers should always be scrutinized before picking up and answering. If it’s important, they’ll leave a voicemail. Yes, some people will leave harassing messages, too. If you don’t respond or make mention of these messages, no one will known. This will prevent people from getting the satisfaction of knowing they’re getting to you.

Fifth:
If you’ve the money and time, change your phone number to a new, private and unlisted one.

Sixth:
Get your mail ASAP. The longer you leave your mail in the mailbox, the sooner someone may snap it up for nefarious means. Always get your mail.

Seventh:
Don't open letters or packages you don't recognize. If you didn't order or request something in the mail, don't risk it. If you suspect something, open all packages and letters over a plastic container large enough to house the item you suspect. While wearing gloves, eye protection and a face mask, ensure the item is being openly as carefully as possible. Record and save everything in case of issue.

Eight:
Look over this PDF, as it provides pertinent information on how to remove your data footprint.

Finally, get off the blogs and stop saying things online. It's better to lurk and learn instead of interacting and putting yourself into danger.

Afterword

And so ends the Paranoid's Bible.

No matter what you do, as long as you read this and the other PDFs/guides in the "Blue primer" you should be fine from citizens. You won't be able to outsmart the government and your more tech savvy corporations. This guide and the ones found in the blue primer are meant to help you prevent spying from the average internet user—to prevent dox.

We'll make more PDFs/guides that'll help you lessen even more of your data footprint and lower your chances of being spied on, however, for now… worry about the citizenry hunting you down like it's the Salem Witch trials all over again.

Questions and Answers

Q: Couldn't Pedophiles use this to hide?
A: Pedophiles already use similar tools and actions to hide themselves and their information. We're simply trying to provide you with the same advantage.

Q: Can't Racists, sexists and other bigots use this?
A: Yes, they can. Why not you?

Q: Won't this allow people to dox others?
A: And…? This information is commonly shared, constantly. We simply scraped the Internet and all it holds to provide you with this information in one place. If you're so worried, share and distribute this guide and its supplementary guides. People can remove their "dox" and avoid any issues.

Q: But isn't transparency key to a happy society? Isn't this hypocritical?
A: Don't use this guide then. You're not the government, are you? Why would you worry about transparency? You're a citizen. You should worry about privacy and security while pressuring the government to be transparent.

Q: What's the worst that can happen, food being sent your house?
A: Sexual aides; Mormon or Muslim missionaries; magazine subscription; identity theft; someone being unstable enough to escalate it into physical harm; Tumblr; Feminists; past abusers; NSA; FBI; Swatting; Scientologists; Surprise Furry…ETC

Q: Will you ever make a guide for UNIX or Linux or whatever it's called?
A: Most of us have lives, jobs, studies or other personal responsibilities. We'll try to get to it when we can.

Q: This guide is to US-centric!
A: This guide was made with US citizens in mind. Most of its information can be applied to citizens of non-US countries. We'll work on other similar PB's when we have the time, research and material.

Q: I knew this already!
A: And others didn't.

Q: Why not sell this information?
A: We are giving it away, for free, because it's just a repository of information readily available online. It isn't 100% our work or knowledge. Why make money off of someone else's work?

Q: How updated will this be?
A: As much as possible for us.

Q: Can I contribute information?
A: Sure! Just let us know what you wish to contribute, what pseudo-name you wish to go by in the "Contribution" page, and give us as much information and research (links…etc) as possible to backup what you wish to provide.

Q: I have found some opt-outs; can I share them with you?
A: Yes! We'd appreciate any information you can provide about opt-outs we missed or new sites to opt-out of. The more opt-outs provided the less information online.

Q: Couldn't terrorists use this to hide their plans?
A: They already do, why not have the information for yourself too?

Q: I'm with the government and—
A: Provide a time stamped and dated image with today's news paper, proof of position, and a homemade ham sandwich.

Q: As a part of Gamergate, I wish to say tha—
A: You're welcome, but this applies to any and all groups online…even if Ghazi or a Literal Who uses it to remove their information.

Q: What about a testament (supplementary guide) about paranormal defense?
A: Provide us with proof of the paranormal and the head of a cryptid and we'll consider it.

Q: What about a testament (supplementary guide) on proper disposal of religious objects?
A: Too varied and too complicated at times. Maybe one concerning a common religion like Christianity and its sects?

Q: A guide to dumpster diving?
A: Couldn't hurt, we'll see.

Q: The Paranoid's bible is too complicated!
A: We're working on refining it.

Q: Wouldn't opting out of sites and databases provide them information?
A: Most likely they already have your information. Think of opting out of these places as acknowledging a contract they have with you already. You're simply taking advantage of it and stating "Well, alright, but remove my information now." That's all opting out does—you acknowledging they have your information and you wanting it removed or withheld from the Internet and prying eyes.

Q: I think this information is very limited and laughable.
A: We're doing the best we can with our extremely tight schedules. You can provide more information and address where something went wrong.

Q: I've witnessed a spelling error or improper grammar.
A: Oh dear lord, please tell us where! We'll fix it ASAP!

Q: A link is dead!
A: What is the link? Do you know of a secondary source to replace it or if it's a simple error like a missing character? What about an archive to replace it with?

Q: Why are you so paranoid?
A: Why aren't you?

Q: Could this be applied to active military personnel or people working the law force or in the government?
A: Yes, but realize that the government offers the above individuals, sometimes, special steps and programs that they can take or participate in to help further remove their information from the Internet. Please consult your Human Resources department or ask someone above you about what you can do. Possibly it was already addressed VIA a memo or manual. Some sites, though, offer an easier route to take to expunge your information for simply being related to someone who's classed as a law officer, military personnel or a government employee.

Q: Isn't this information illegal?
A: Truthfully, at the most, it's a legal grey area.

Q: Can't people use this information for illegal purposes?
A: It's all up the reader, we just made it available.

Q: What prevents them from not following through with the requested opt-out?
A: Various DPPA and GLBA laws, besides several other items.

Q: Won't this prevent background checks and limit your job possibilities?
A: No. It will not. This simply scrubs the information and hides it from the public's eyes. Many background checks demand you sign a release per FCRA guidelines. No one can legally run an investigative search on you without your express permission. You also will have to realize that all legitimate, legal background checks (for hiring purposes) are not only paid for but go through the proper government channels, not some data miner's site.