

Attachments

When viewed electronically, this document is **best viewed in Adobe Acrobat or Reader**, because it comes equipped with a series of **embedded/attached guides** for navigating settings on different devices and software. **The attached guides are designed for you to print them two-sided.**

The Complete Privacy Checkup Checklist

[Social Media Settings Guide](#)

[Privacy Settings Checklist](#)

[Configure Firefox to Reduce Tracking](#)

[Configure Brave to Reduce Tracking](#)

[Configure and Use Signal Messenger for messaging, voice, and video calls](#)

Harden Devices and Reduce Tracking:

[iOS/iPadOS Devices](#)

[Android Devices](#)

[Windows PCs](#)

[MacOS Computers](#)

[Database Removal Checklist](#)

Organization

This Checkup has three parts:

Part I briefly discusses what information is collected on you, how it is collected, and how you are tracked.

Part II is the **complete digital privacy Checkup**. It supplies practical steps to harden yourself, reduce data collected on you, and reduce tracking. If you just want to get right down to improving your privacy, [skip to this section](#).

Part III provides you information on extra steps to take when traveling with a special section on travel to high-risk countries like China.

Some of what you are about to read will be surprising to you. It might make you want to hide under a rock. This Checkup's goal is not to convince you to go off-grid. Its goal is to make you aware and give you some tools to significantly reduce the amount of information collected on you and confuse methods used to track you.

IT IS ALL ABOUT ARTIFICIAL INTELLIGENCE

Data collection is not new. Companies have been collecting detailed information on their customers for as long as there have been companies, but **two things have changed: 1) the scale of data collected, and 2) the ability to analyze it effectively.** First, scale. The amount of data stored – the sum of stored information from humans – now doubles about every two years, and that pace is accelerating. Second, analysis. Only a few years ago, a human analyst would have to painstakingly piece this information together, which would require a lot of time, ability, and motivation. In most cases, it was not worth it. Today, increasingly sophisticated artificial intelligence algorithms, combined with unprecedented computing power, give companies and governments the ability to rapidly sift through enormous datasets with millions of data points to draw detailed and nuanced conclusions. Conclusions that humans would not have been able to make with the same data. It should come as no surprise that some of the companies (e.g. Google, Amazon) and entities (e.g. China) most invested in collecting vast volumes of information are also those most invested in computing and artificial intelligence capabilities to effectively analyze the information they collect. The popular artificial intelligence branch known as machine learning also requires large datasets. **The result is an international arms race to collect and aggregate the most data.**

Today's artificial intelligence algorithms can do amazing things – translate foreign language accurately on-the-fly, provide accurate transcripts for phone calls and meetings, recognize billions of faces (even if obscured, or from twenty years ago), and even generate completely fictitious but realistic videos. You probably use AIs regularly in the form of digital assistants like Apple's Siri, Ok Google, Amazon's Alexa, or Microsoft's Cortana. Here are some public examples of the current state of artificial intelligence capabilities:

- **How a Chinese AI Giant Made Chatting—and Surveillance—Easy** (<https://www.wired.com/story/iflytek-china-ai-giant-voice-chatting-surveillance/>) - while the other examples here are civilian and not directly associated with surveillance, this article offers a peek behind the curtain by discussing how China uses commercial data to fuel its state surveillance AI algorithms.
- **How Machines Learn** (<https://www.youtube.com/watch?v=R9OHn5ZF4Uc>) – a short YouTube video by CPG Grey giving a basic explanation of how machine learning works.
- **This Person Does Not Exist** (<https://thispersondoesnotexist.com>) – a website that generates photo-realistic photos of people who do not actually exist, and without using any information from actual photos.
- **Talk to Transformer** (<https://talktotransformer.com/>) - when you provide a starter sentence/prompt, this website generates a realistic but fictitious news article from it.
- **Google AI Experiments** (<https://experiments.withgoogle.com/collection/ai>) – a collection of AI demonstrators and experiments.
- **IBM Project Debater** (<https://www.youtube.com/watch?v=kjpFcMfMW9c>) – clips from a video debate between a world champion and IBM's Project Debater, an AI that generates detailed, logical arguments in the debate competition format on-the-fly.

SOME OF WHAT IS COLLECTED ABOUT YOU

Social Media Information: This one is obvious. You are likely aware that social media companies are in the business of making money off you and your information. They are free services because your data is valuable (and they are not alone – you probably also use free email and other services that profit from your data). First, they compile information on you based on your behavior, activity. First, they compile information on you based on your behavior, activity, *information you and others provide*, and conversations on the service and share it with advertisers (which can be anyone willing to spend a few ad dollars). But social media companies like Facebook (which includes Instagram and WhatsApp), Microsoft (LinkedIn), Snapchat, and many others, are not the only ones collecting your social media data. Public information from these platforms is often the first-place nefarious actors – ranging from burglars to foreign intelligence organizations – go to collect information on you, often in an automated fashion. Just your profile picture, which is always public on Facebook, can be valuable – it can enable facial recognition and tracking, and someone can analyze the picture’s metadata to find where you took the picture. That might be your home. But many people have much more data publicly available on social media – resumes, personal histories, political discussions and opinions, and family photos. And if you don’t have any useful public information on social media about you, chances are someone in your circle of family or friends does – they posted a photo from your birthday, which tells everyone what your birthday is, or talk about how great a Special Forces hero you are.

How to reduce it: social media privacy settings and careful use

Public Information: Public databases include things like title records and property tax records, which may indicate where you live and what you paid to live there. These records vary by where you live. While there may be things you can do to reduce this information, in most cases, it’s out of your control. This category also includes information about you publicly available on the internet, like old news articles or blogs. You may be able to do something about old websites by contacting the site owner, especially if it was owned by you, and having it taken down. Regardless of whether you can control what is publicly available about you or not, you should be aware of what is out there because it will be combined with information obtained from the other sources discussed here to build a profile on you.

Public information also includes information compiled and available for sale by “people finder” sites like PeekYou, Pipl, Spokeo, WhitePages and many others. These data brokers scrape public databases and the web, including public social media information, to build full profiles on everyone, making them available for a small fee to anyone willing to pay for them. While these sites all offer opt-outs, if you don’t stop the data at the source, they will repopulate your profiles in only a couple of months.

How to reduce it: awareness and contacting site owners, opt-outs (see [Database Removal Checklist](#)).

“Shared” Data

If you read a lot of privacy policies, one thing will stick out. **Some of the worst companies with respect to privacy can truthfully claim they don’t sell your data.** Instead, *THEY SHARE IT* – with service providers, processors, partners, and yes, advertisers.

Your data is the incentive for advertisers to place ads on their service. Or it is part of a data sharing agreement between two companies interested in collecting more data on you (like social media companies and credit bureaus).

Theft from Private Databases and Accounts: Chances are you have experienced some form of fraud or data theft in the last year or two. It is incredibly common. Hackers steal data regularly, especially from major data aggregators (e.g. 2017 Equifax hack, or the 2014 eBay hack). State actors like China are often the suspected culprits, but sophisticated independent criminal groups also conduct regular data heists. In many cases, thieves put stolen data up for sale in online black markets. Stolen data often includes stolen usernames and passwords. Thefts are not always major – hackers guess weak passwords with automated tools every day to steal money and data from online personal accounts or stolen devices. While you cannot control what data hackers steal from companies, you can reduce the amount of data companies have on you to steal in the first place, while also preventing would-be thieves from breaking into your personal accounts.

How to reduce it: strong passwords, two factor authentication, password managers, encryption, breach monitoring, and changing passwords from the default on routers and internet-of-things-devices (e.g. cameras), privacy settings/opt-outs, and choosing more-private alternatives that collect less data.

Web Browsing: Advertisers, internet service providers, device makers, and others track your web browsing activity and internet searches through multiple methods. Your browsing activity tells them about your interests, including sensitive interests and planned activities. In the U.S., a 2017 law (S.J.Res. 34) allows internet service providers to collect and sell this information without your approval, but they are only one group of many collecting and selling or sharing this data – Google is the largest collector of them all.

How to reduce it: browser settings and plugins, VPNs, encrypted DNS, disabling tracking cookies, and using a private search engine

Media Consumption: Your smart TV and the services you use (e.g. Netflix, Hulu, Spotify) log your media viewing and consumption habits. The companies behind these devices and services share or sell this data to data brokers, advertisers, and even credit bureaus.

How to reduce it: privacy settings and opt-outs

Financial Information: You know that your financial institutions report information to credit reporting agencies (CRAs) like Equifax. You also know CRAs know a lot about you – your income, credit history, and even what kind of car you drive. You might be surprised to learn that CRAs also aggressively collect and buy data from other sources to build a more complete profile on you, including social media information, web browsing activity, and media consumption. Your financial institutions and credit card processors (e.g. Visa, Mastercard) may also sell or share information on your spending habits to anyone willing to buy it, or they share it with partners. While they usually “anonymize” this data, it can be easily combined with other openly available information to identify you and your spending.

How to reduce it: credit freezes, opt-outs/privacy settings, use cash or more-private alternatives (e.g. Apple Pay/Card).

Your Cell Phone Use: Your cell phone company collects information on your phone and SMS use and your phone’s location (your phone broadcasts its exact location to the company through what towers it uses). All this information is available to them and companies they may sell it to or share it with. Additionally, calls and texts can be easily listened to and read by the company, its employees, a government requesting it, or hackers who have gained access to their networks, which suffer from notoriously poor security. In fact, through the shared international Signaling System 7 (SS7), which allows companies to provide service to out-of-network phones, any cellular company anywhere, or anyone with access to SS7 anywhere, can tap a phone call, read SMS messages, collect phone locations, your contact list, and can potentially use the system to gain malicious access to your phone.

How to reduce it: use encrypted services (e.g. Signal, iMessage/Facetime), Wi-Fi calling

How and Where You Use Your Devices: Modern smart devices, especially phones and tablets, are surveillance devices. Both the devices themselves and the applications you use track and report your activities. If you share your location with an application, then your location is also shared with the application's creator (most of the time). Some applications (e.g. Facebook) even collect information on *what you do on other applications* and many more applications collect data on your device, like what applications you have installed. Windows computers by default also collect significant information on your activity. If you use Apple devices, they collect a lot less data compared to competitors' devices, but still collect quite a bit of data.

How to reduce it: device, app, and account privacy settings

Your Communications and Stored Data: Many communications services collect detailed information on who their users communicate with, when they communicate with them, and often even the content of conversations (both in text and over voice/video using advanced artificial intelligence capabilities). This includes message and phone services like Skype, WhatsApp, or Facebook Messenger, as well as popular email services like Gmail, Yahoo Mail, or Outlook.com. Google even tracks your purchase history by scanning your Gmail emails, and the others engage in similar practices. Of the examples given, only WhatsApp does not collect information on the content of conversations. If you store information with a cloud storage provider like Google Drive/Docs, Dropbox, Apple's iCloud, or Amazon Web Services, the cloud storage provider collects information on what you store, how you store it, and has full access to view and collect information on the content of your files and photos. You are entirely beholden to their changing privacy policies.

How to reduce it: account privacy settings, and choosing privacy-oriented alternatives (such as Signal Messenger, ProtonMail or Posteo for email, and Sync for Tresorit for cloud storage)

How and Where You Drive Your Car: Yes, even your car is not safe anymore. All late-model cars come equipped with sophisticated computers, hundreds of sensors, and cellular modems that track and report everything you do. Car manufacturers now collect information about where you go, how fast you go to get there, how many people are in the car (and what they weigh), and how aggressively you drive. If you connect your device to the car's computer either by Bluetooth or USB, then your car manufacturer will also collect information on your device, how it's used, and most will also vacuum up your full contact list and SMS messages. They sell this information to insurers, data brokers, traffic monitoring services, and others. Rental car companies install added sensors to collect even more data on you. In many cases, your car can also be tracked using cameras that read and log license plates or that read toll pass information, but there is not much you can do about this besides being aware of it.

How to reduce it: privacy settings and opt-outs; avoid connecting device to cars, especially rental cars

Much, Much More: Various groups collect other data from many other means, including closed circuit cameras (e.g. facial recognition), smart home devices, and more.

HOW YOU ARE TRACKED

You can draw some conclusions about how you and your activities are tracked from the previous discussion on what information is collected on you and from where. The good news is that you can completely prevent/stop most of it (see Part II). As with the information discussed above, even if you trust these companies with your data, it is out of your control and prone to theft from malicious actors.

HOW YOUR ACTIVITY IS TRACKED ON THE INTERNET

Advertisers, service providers, governments, and others can track your activity on the internet through multiple means:

- 1) **Your Internet Service Provider/Cellular Provider:** Your internet service provider, which includes your cell phone company when connecting to the internet through a cellular connection, can see two things: 1) Your visits and interactions with unencrypted websites, and 2) what encrypted sites you are visiting (but not what you are viewing there). Of course, your service provider knows it is you because it is providing you the service. **Encrypted websites are denoted by the S in <https://>** in the web address, and often by a lock icon next to the address in your browser. If you have never changed your domain name system (DNS) settings, or ever heard of them, then chances are your DNS requests also all go through your provider, and even if they don't, they are not encrypted. Practically, what this means is that every time your browser or device "requests" to visit a website, your service provider processes the request and points your browser/device to it. So even if the website is encrypted, your provider knows you went there because it processed the request.

Stop it: browser/device settings, browser plugins (HTTPS everywhere), encrypted DNS (Cloudflare 1.1.1.1), and/or a VPN.

- 2) **Public Wi-Fi Networks:** When you use public Wi-Fi networks like at a hotel, airport, or coffee shop, the company hosting the network can see detailed information on the device you are using that can uniquely identify you (you may also have to enter your name and contact information to use the network). Like with internet service providers above, they can collect detailed information on unencrypted web browsing, or what encrypted websites you are visiting. Criminals can collect the same information by setting up fake public networks.

Stop it: use a VPN, and consider using a mobile Wi-Fi router/bridge, which will conceal the identifying information of your devices from the public network and put them behind a layer of security

- 3) **Browser Fingerprinting:** When you visit a webpage, your browser communicates a lengthy list of information to the website about your computer or device and your browser. The information includes things like what browser and version it is, your screen resolution, the default language, and what fonts you have installed. Your browser sends this information so the website knows how to display itself to you. However, in many cases, this information, when put together, is completely unique to your device. Like with tracking cookies, because major advertisers can collect this information across most of the internet, they can accurately identify you and track your browsing activity. You can test your browser's fingerprint at Panopticlick: <https://panopticlick.eff.org/>

Stop it: use a privacy-oriented browser (e.g. Firefox, Brave), virtual machines (advanced)

- 4) **Third-Party “Tracking Cookies”:** If you have used the internet, you have heard of cookies. Many of them serve an important purpose, like those that tell a website you have already logged in so that you don’t have to do it every time you visit. However, most websites today also harbor third-party tracking cookies. Major advertisers embed these cookies and use them to track your browsing activities across different websites. Because there are only a few major internet advertisers, like Google’s DoubleClick or Facebook, these cookies provide detailed information on all your browsing activities. You can also be uniquely identified through your browser and system information (see browser fingerprinting above).

Stop it: browser settings (disable third party cookies), and browser plug-ins (Privacy Badger and uBlock Origin).

- 5) **Your Search Engine:** Chances are you use Google. Google logs and tracks all your searches, keeping a detailed search history that allows it to tailor results for you, and to collect information on your interests to share with advertisers. Google also tells the websites you visit what you searched for to get there. Google combines this information with information it collects on your browsing through its DoubleClick ad network and website analytics services, which underpin most websites you visit (see browser fingerprinting and third-party tracking cookies, above). You probably also use Gmail, which tells Google what you spend and where and much more (who you talk to and when and what you talk about). Together, this information provides Google with complete information on everything you do online.

Stop it: switch to a privacy-oriented search engine like DuckDuckGo or Startpage

HOW YOU ARE TRACKED IN THE REAL WORLD

As discussed above, there are many ways your location/movement may be tracked, but this section will focus on what you can affect:

- 1) **Cellular Location:** As discussed above, your cellular devices continually report their exact location. Unfortunately, there is not much you can do about this besides turning off the device’s cellular antenna when you don’t want to be tracked. For most people, that is impractical.
- 2) **Device and Application Location Sharing:** By default, your devices – including iPhones and iPads, Android phones or tablets, Macs, and Windows computers – regularly report their location to the manufacturer. If you share your location or enable location sharing with an application or service on any device, then that application also regularly collects and usually logs your location. This is the easiest way for advertisers (and those posing as advertisers) to track and identify you, as application makers routinely sell it and it is widely available.

Stop it: Reduce/stop location sharing, account privacy settings

- 3) **Wi-Fi/Bluetooth Fingerprinting:** Your devices continually broadcast the names of known Wi-Fi networks (SSIDs) as they search for known networks to connect to. This sometimes-long list of networks your devices have connected to can be used to uniquely identify and “fingerprint” them. Retail stores and other public settings may pair this capability with beaconing (#4 below) to identify and track you. Local hackers can use the same information to snoop on your device by naming a fake network after one you have connected to, thus forcing your device to automatically connect to it. Additionally, many applications report the name of the Wi-Fi network your device is connected to, as well as the names of nearby networks (they can no longer do this on Apple devices as of iOS13). Since Wi-Fi networks are well-mapped

(see www.wifimap.io or www.openwifimap.net), this unique set of nearby Wi-Fi networks can be used to physically locate you as well as track where you have been. Information from your devices' Bluetooth broadcasts can be very similarly used to uniquely identify you (you are the only person routinely in range of the same Bluetooth beacons).

Stop it: forget/delete rarely used Wi-Fi networks after using, turn off Wi-Fi and Bluetooth antennas when not in use, device/account privacy settings (certain location services settings; disable location history)

- 4) **Wi-Fi/Bluetooth Beacon Tracking:** As you walk about a store or public area with your device's Wi-Fi and/or Bluetooth antennas turned on, retailers and others can very accurately track your movements. Modified routers around the space detect your device broadcasting in search of Wi-Fi networks or Bluetooth devices to connect with. They use this information to triangulate your location. When combined with Wi-Fi/Bluetooth fingerprinting, retailers use this information to identify you and collect information on your shopping habits. In some areas, authorities also use this technology as part of so-called smart or safe city capabilities to identify and track you for law enforcement and surveillance purposes. This has recently taken on new importance with COVID-19 contact tracing apps, which log these beacon encounters as a record of you being in proximity to others (other apps do this for other reasons). Consequently, if you are wearing Bluetooth devices or have turned on Bluetooth on your phone in public, information from these apps can potentially be used to track you even if you don't download the app yourself. Similarly, by default, your devices continually provide Apple and Google with information on nearby Wi-Fi networks and Bluetooth devices.

Stop it: turn off Wi-Fi and Bluetooth antennas when not in use, device settings

OTHER RESOURCES

For more information on who collects information about you, how they track you, and what you can do about it, these resources offer excellent information:

- 1) **The New York Times Privacy Project** ([nytimes.com/series/new-york-times-privacy-project](https://www.nytimes.com/series/new-york-times-privacy-project)). A long series of articles illuminating the various aspects of modern surveillance and privacy threats, along with some guides.
- 2) **The Electronic Frontier Foundation (EFF) Surveillance Self-Defense Guide** (ssd.eff.org). EFF is a privacy advocacy non-profit, and its Surveillance Self-Defense Guide supplies dozens of tutorials and guides to increase privacy and harden communications.
- 3) **Shoshana Zuboff on Surveillance Capitalism | VPRO Documentary** ([youtube.com/watch?v=hiXhnWUmMvw](https://www.youtube.com/watch?v=hiXhnWUmMvw)). A 50-minute documentary based on an interview with Shoshana Zuboff, a Harvard professor and author of the book *The Age of Surveillance Capitalism* (also worth reading). It will help you understand how extensively advertisers and tech giants track you, and how they use the data they collect to target you.

ANOTHER POSSIBLE FUTURE?

This Checkup focuses on self-defense for our current privacy crisis. But there is hope. New decentralized technologies offer an alternative digital future where data is private, secure, and owned by everyone – technologies like blockchain (the underpinnings to Bitcoin), directed acyclic graph (DAG) projects like IOTA (similar but without the massive energy requirements), and new communications protocols like [matrix]. Together, these

technologies and others could completely disrupt and overthrow every one of today's data monopolies and pass digital power back to the people – us – who produce the data. **But that future will not happen without people retaking ownership of their privacy, and making deliberate consumer choices to usher it in.** This Checkup will help you start.

Part II: The Complete Privacy Checkup – Take Charge of your privacy

If you read [Part I](#), you understand how daunting the challenge of rebuilding your privacy is. Either way, you are here because you are ready to take charge of your privacy. This section discusses issues topically, but it is more efficient to work through the Checkup actions in a different order. To make it easier, the attached [Complete Privacy Checkup Checklist](#) walks you through the Checkup actions in task order. If you struggle with any of the steps, ask a technically minded friend or relative to help. We are all in this together.

☐ FIRST, CARE ABOUT PRIVACY

Checkup Action:

☐ Become engaged in privacy issues.

Privacy has eroded because people have allowed it. Every consumer choice you make is a decision on privacy. In many cases, you and others have chosen free services over paid ones, and the cost has been your privacy. **With so many of us making the same choices, this has left the current state of privacy in crisis.** For some markets, there are no longer any readily available privacy-friendly alternatives. It also means many of us have become complacent about our privacy – resigned that we are helpless to do anything about it.

As you will see, **there is a lot that you can and should do**, but much of it falls short because of a lack of strong privacy laws and consumer protection. While some jurisdictions, like California, or Europe, have better privacy regulations than others, they are all significantly lacking and require consumers to actively opt-out of most data collection. **Most Americans don't have a legal right to most of their data.** Consequently, the best thing you can do for your privacy is to advocate for it. Support privacy causes. Contact your legislative representatives and choose products that favor privacy over consumer surveillance.

☐ BECOME A SETTINGS NINJA AND EXERCISE YOUR PRIVACY RIGHTS

Checkup Actions:

- ☐ Complete device settings checklists for your devices ([iOS/iPadOS](#), [Android](#), [Windows](#), [MacOS](#)).
- ☐ Comb through device, account, and service settings to restrict data-sharing, following the [Privacy Settings Checklist](#).
- ☐ California and European Union Residents (...or those pretending to be...): exercise your right to request companies not sell your data for the services you use.
- ☐ Place credit freezes at Experian, Equifax, and TransUnion.
- ☐ Use a breach monitoring service (e.g. Firefox Monitor).
- ☐ When you have completed everything in the Checkup, consider completing the [Database Removal Checklist](#) to start with a clean slate.

You need a new habit to help you become a Privacy Settings Ninja: the first thing you should do when you get a new device, create a new online account, or download a new application is comb through the settings. Assume any claims that they anonymize your information are false (see [footnote](#) on page 3). When reviewing settings, look to disable any sharing or collection of data that does not seem completely necessary for the service to work. Where to find the right settings varies from service-to-service; you are looking to do a few things (not all of these are always available):

- Disable targeted advertising and ad tracking (sometimes called “opt outs”)³
- Disable location tracking and history/logging
- Disable/opt-out of “analytics” or “help us improve your experience” data collection
- Disable/opt-out of the sale of your information
- Disable/opt-out of anything that looks or sounds like data collection (look for trigger words: “log,” “record,” “collect,” “store,” “analyze,” and features that “suggest” things for you)

Location Services:

Location Services (on Apple devices), also known as Location Sharing on Android devices, is a lot more than just your location. When agreeing to location sharing, you are agreeing to share your GPS location, cellular tower information, names and signal strength of nearby Wi-Fi hotspots, and identification and signal strength of nearby Bluetooth devices by default. None of this data stays on your device – it all gets sent to the application’s company, which may sell or share it with others.

Only allow location sharing with extreme discretion. Ideally, you can live without it altogether.

³ On many websites, you will see options, such as in privacy policies, to opt-out of targeted advertising based on cookie tracking. **Don’t do it.** Ironically, they opt you out of tracking cookies...by placing a tracking cookie on your system. Instead, [secure your browser](#) from these cookies altogether.

- Be incredibly careful about what applications you choose to give access to your location, contacts, calendar, microphone, camera, photos, and other data on your devices. You should assume that most services requesting this access will collect, misuse, and sell or share it.
- Enable two-factor authentication, or added authentication measures (more on this [later](#))

You also need to **check settings on both your mobile devices and on the service's website** – the two often offer different options (with the website usually giving you finer control over your privacy). Also, don't just restrict your search to settings labeled under "privacy." Companies often hide data-exposing settings in other menus.

Once you have comprehensively reviewed settings for all the applications, devices, and services you use, you also need to **periodically recheck them**. Services change their settings regularly, so look for new options.

See attached guides for going through this process on [iOS/iPadOS](#), [Android](#), [Windows](#), [MacOS](#), as well as the [Privacy Settings Checklist](#). If you live in more privacy-friendly jurisdictions, like California or Europe, you may find you have more options available to you...

KNOW YOUR RIGHTS (OR PRETEND YOU HAVE SOME...)

If you live in the United States, you may be surprised to learn that you don't own your data – not your emails, social media posts, or any of the information that you provide to a company. Such is the sad state of privacy in the U.S. – websites and services can lawfully keep the data they collect from you indefinitely in most cases.

"If you live in the United States, you may be surprised to learn that you don't own your data – not your emails, social media posts, or any of the information that you provide to a company."

There are two exceptions: California and Nevada Residents. As of 1 January 2020, residents of California have three fundamental privacy rights under the **California Consumer Protection Act (CCPA)**: (1) the right to request copies of their data in a common format, (2) the right to request a company not sell their data, and (3) the right to delete their data on request (with some exceptions). Nevada residents only have the second right – the right to request companies not sell their data. Importantly, you must opt out for every service/company – by default, most will still sell your data. Companies also don't have to make it easy to opt-out.

European Union residents have similar (if slightly more robust) rights under the **General Data Protection Regulation (GDPR)** as residents of California. Under the GDPR, you must opt-in to sales of your data, and can revoke your consent at any time. However, unlike the CCPA, the GDPR is geographically limited and may not apply if you are using a service without operations in Europe or if you are not in Europe.

If you are not a resident of California or the European Union, you may still have some luck exercising these rights. Some companies have extended these rights to all their users – the tech giants, such as Google, Apple, and Microsoft, mostly fall into this category (they want to avoid stricter legislation, and they could change those rights tomorrow in their privacy policies). You may also have some success if you pretend to reside in these places (particularly California). Try using a VPN server located in California or Europe and see if the website gives you different options (more on VPNs, [below](#)). You can also try pretending to be a Californian. Many services don't require any proof (like an address) beyond certifying you are a California resident. They are unlikely to verify the

information. You can easily have addresses on file elsewhere and still be a California resident and in most cases, there is no penalty for lying.⁴

How to exercise your rights (...or pretend rights): If you don't see the choice to opt-out of the sale of your information, request your data, or delete your information readily in the settings, **scroll all the way down to the bottom of the page**. 95% of the time, at the bottom you will see a link to their "Privacy Policy" or "Data Policy." Don't worry. Unlike user agreements, these are usually short – a couple pages. Reading privacy policies is a good habit to get into, because they will explain, often very clearly, what the company collects, how it collects it, and how they use it. If you read a lot of them, you will quickly be able to tell what companies truly value your privacy. The privacy policy will explain how to exercise your rights (look for "your rights," or CCPA). You will usually need to fill out either an online form or send an email with your request.

The websites DeleteMyData (deletemydata.io) and justdeleteme.xyz provide by-company information on how to go about deleting your account and data. Companies/sites marked impossible in these two resources must usually still follow the CCPA if they have operations in the U.S. If they say they don't delete accounts/information, tell them you are reporting them to the California Attorney General for violating the CCPA. They may change their tune. If you really are a California resident, you should report them here: <https://oag.ca.gov/contact/consumer-complaint-against-business-or-company>.

ANOTHER RIGHT: CREDIT FREEZES

All Americans have the legal right to request credit freezes at the major credit bureaus for free (bureaus may sell a similar credit "lock" feature – don't waste your money). It is an effortless way to prevent someone from stealing and using your identity. With a credit freeze in place, no one can open a new line of credit or request a "hard pull" of your credit without you first lifting the freeze. You just need to remember to temporarily lift the freezes before shopping for a new loan or credit card. **To put freezes on your credit:**

- **Equifax:** <https://www.freeze.equifax.com>
- **Experian:** <https://www.experian.com/freeze/center.html>
- **TransUnion:** <https://www.transunion.com/credit-freeze>

You should also consider a credit or breach monitoring service. Firefox Monitor (monitor.firefox.com) allows you to search databases for stolen account information by your email addresses to see what accounts, and often passwords, have been compromised. If you sign up for a free account, Firefox Monitor will also send you notices when it finds your email addresses in a new breach. Most paid identity protection services also offer this feature on top of credit monitoring – probably the most economical (and still excellent) option for users of this guide is Dashlane Premium Plus (dashlane.com), which gives you an excellent [password manager](#) and full identity protection service for \$10/month. Dashlane offers just the password manager and breach monitoring for its Plus accounts at \$5/month.

⁴ **A word of caution:** Some web forms may use the words "I attest under penalty of perjury that I am a California resident..." If the form includes those words and you agree, you could be committing perjury under California law (if you aren't actually a resident). If it does not contain those words, then there is no legal risk for pretending to be a Californian (for non-government matters, the law requires those words to be in the agreement). So, do this at your own peril. The odds that any company would take the time to collect proof that you are not a resident and pursue legal action is absurdly low given that no meaningful amount of money is involved, but if you don't want to break the law, then don't "attest under penalty of perjury."

☐ LOCK DOWN SOCIAL MEDIA

Checkup Actions:

- ☐ **Double-check privacy settings for social media accounts to restrict public information and sharing. Change any old public posts to private (just friends). See attached [Social Media Settings Guide](#) for a walk-through of Facebook, LinkedIn, Instagram, Twitter, and Reddit settings.**
- ☐ **Check profile photos and replace photos taken in revealing locations with others or delete and replace with an avatar or non-identifying photo.**
- ☐ **Review and delete unnecessary or revealing details in your social media profiles.**
- ☐ **Review your friends and remove suspicious accounts or people you don't know.**
- ☐ **Consider deleting social media apps from your devices and using the website instead (you can still have the icon on your home screen/app drawer).**

Unfortunately, you should probably maintain social media accounts for a few reasons (especially Facebook). They are obviously useful for staying in touch with family and your community and lining up jobs in the case of LinkedIn. More importantly from a privacy perspective, it can be unusual to not have a social media account depending on your age group, which may invite more scrutiny on you from someone inspecting your personal life. Also, keeping a social media account does two things: 1) it prevents criminals and other malicious actors from using your information to create and use an account in your name, and 2) it allows you to watch and gain some control over what people say and share about you on the platform. As discussed in the introduction, not being present on social media does not prevent other people from posting information about you there. While some people might choose to join social media platforms in aliases, or use their middle name, this does not provide meaningful security – a quick analysis of your connections will quickly reveal who you really are (and in some cases, your true name is also in your profile's web address).

But while you might need to have an account, here is what you should do:

- **Comb through the privacy settings to ensure that as little of your information is public as possible and ensure posts are private.** By default, many social media services make your information and what you post completely public. You need to lock this down. Make posts private or visible only to friends. Make it so only friends of friends or people connected to you can find and connect with you. Cut unnecessary information from your profile (birthdays, information on your family, interests, etc.). Hide and restrict access to information on your group memberships. If you don't do this step, anyone with a web browser can compile everything you make available, and data brokers will do this.
- **As with step two, disable ad tracking, location sharing, facial recognition, and user analytics.**
- **Ensure profile photos do not provide information on where you live or work (if they were taken at your house, they likely do), and consider avatars or non-identifying photos for your profile.** On most social media sites, your profile photos are completely public. There is a good chance your photos have embedded location information on where they were taken. If the photo was taken at a private place (your home, work, your friend's, or family's home), then choose another photo, or if you are savvy enough, ensure you check and remove the metadata (which is called EXIF information) before

posting it (Apple photos now offers this as an option when sharing images). If you don't want your image to be public and available for automated systems to take it and enable facial recognition and tracking of you, then post a non-identifying picture.

- Remember that the social media service will collect and analyze anything you post, comment, and the service will sell or share these "insights" with advertisers and others.
- Avoid commenting on posts marked public. As with public posts, anyone with a web browser, and especially data brokers, can collect and compile your public comments. On Facebook (and most services), a public post is indicated by a globe icon.
- Monitor what people post and say about you, and check if it's public. Contact and ask them to restrict access on public posts about you.
- Only accept friend requests from people you know and consider asking them a question only they would know the answer to before accepting. Imposters use fake friend requests to snoop on you and your family, usually for criminal purposes.

THINK ABOUT DELETING SOCIAL MEDIA APPS

Social media apps are known data devourers. They collect information on everything from your phone/tablet that they can – which can include what apps you have installed, what other apps you use, when you use them, etc. While they don't have exclusive rights to this club – many (mostly free) apps are also guilty of this – they're the most consistently likely to be on your device. If you are using the latest operating systems (iOS 13, Android 10), they have "sandboxed" and prevented *some* of this collection, and allowed better user control over app permissions, but the simple solution is to delete the apps and use the webpage instead. There are instructions on how to do this in the [Social Media Settings Guide](#).

☐ STOP INTERNET TRACKING BY RECONFIGURING YOUR BROWSER AND CHANGING HOW YOU SEARCH

Checkup Actions:

- ☐ **Recommended:** install the latest version of Mozilla Firefox and set to default; follow [Firefox configuration guide](#) to restrict tracking. Alternately, install [Brave](#).
- ☐ Complete settings checklist for your browser ([Firefox](#) or [Brave](#)); install browser extensions.
- ☐ Review and delete unnecessary browser extensions.
- ☐ Set default browser to DuckDuckGo or Startpage and start searching privately.

SECURE YOUR BROWSER

A few simple changes to your internet browser can make an enormous difference on advertisers' ability to track you on the web. This guide recommends Mozilla Firefox for its commitment to privacy, ease of navigating settings, and support for extensions. If you have not tried Firefox in a while, give it a shot – it has come a long way. See [attached guide](#) for instructions on configuring Firefox for maximum privacy.

Chances are you use Chrome, which unfortunately, is difficult to get completely private. Even when thoroughly "locked down," it will still report information to Google. A practical alternative to Chrome is the Brave browser, which uses the same source code as Chrome, but is set up for privacy by default (just don't enable Brave Rewards). This Checkup also includes a [Brave configuration guide](#).

This Checkup also strongly recommends you install three browser extensions:

- **Privacy Badger:** By the Electronic Frontier Foundation (EFF), a privacy advocacy non-profit, detects and blocks [tracking cookies](#). (alternatives: Disconnect Private Browsing, Privacy Possum, Ghostery)
- **HTTPS Everywhere:** Also by the EFF, detects if an encrypted version of the webpage you wish to visit is available and automatically upgrades you to the encrypted version. (not needed on Brave, which does this on its own)
- **uBlock Origin:** Detects and blocks ads and ad-based trackers. (alternatives: NoScript, ScriptSafe)

A Warning About Browser Extensions:

Browser extensions like these can be incredibly useful, but they can also make you easier to identify. Installing a long list of extensions can make it easier to [fingerprint your browser](#). You should carefully review the extensions you have installed and delete unnecessary extensions. Certain extensions are also designed to track you (e.g. Rakuten, Amazon, Google extensions) and you should avoid them.

CHANGE YOUR SEARCH HABIT

You should also change how you search for information on the web. Google records your searches and reports them to the sites you visit and combines that information with information it collects through its internet surveillance network (DoubleClick and Google Analytics) and other information it collects from your (Gmail, Google Drive).

To avoid giving one company such complete information, **this guide recommends you switch to a privacy-oriented search engine: DuckDuckGo or Startpage.** Neither of these search engines record your searches. DuckDuckGo provides excellent results from its own search engine and does not report your search terms to the websites you visit. Startpage conducts an anonymous search using Google's search engine and provides you the results, and offers an "anonymous view" option, which shows you the page without you visiting it (Startpage is retrieving it for you), concealing your information from the website.

☐ HARDEN YOUR ONLINE ACCOUNTS WITH A PASSWORD MANAGER, STRONG PASSWORDS, AND BY ENABLING TWO FACTOR AUTHENTICATION

Checkup Actions:

- ☐ Set up and use a password manager (Dashlane, LastPass, 1Password, KeyPassXC), using a strong diceware password and enabling two factor authentications to protect it.
- ☐ Review your existing device and account passwords:
 - ☐ Set strong diceware passwords or use your password manager to generate and store strong passwords.
 - ☐ Enable two factor authentications where available, favoring software tokens (e.g. LastPass Authenticator) - optional extra-security: hardware tokens.
 - ☐ Watch out for security questions; consider giving fake answers.
- ☐ Take this opportunity to delete any old or unused accounts (DeleteMyData.io).
- ☐ Avoid single sign-ons (e.g. login with Facebook, Amazon, or Google) – Apple single sign-on is okay.

SETTING AND MANAGING STRONG PASSWORDS

Like most people, manic network administrators have trained you to think a complex password looks something like this: %aVd9Jzhs@_HLacU02#. That is undeniably a complex and strong password, but can you remember it, along with the 30 other passwords you use regularly? Probably not. Because of this situation, many people re-use the same passwords repeatedly for different sites, or use common “complex” passwords that a computer can guess easily (chances are it’s one of these 50,000 most common passwords: <https://mozilla.github.io/application-services/docs/accounts/50000-most-common-passwords.html>, or otherwise appears in common leaked password databases). The result is a security catch 22: computers, which can guess millions of passwords a second, can easily guess common or simple password and re-using passwords on different sites means if hackers steal your password from one site, then they have stolen your password for many sites.

You need two tools to break this impasse: a password manager and a complex, easy to use password – a diceware password.

Password Managers: First, a password manager is not a piece of paper on your desk or a note on your phone. Thieves can easily steal both paper and digital notes, compromising every account you have. A password manager is an encrypted database that securely stores all your passwords. You set a single complex password, and let the manager do the rest. The password manager generates long, complex, and unique passwords that fit the requirements of the various sites and accounts you use, and all you need to remember is your one password for the password manager itself (you also want to protect it with two factor authentication, below). Many password managers, like Dashlane (<https://www.dashlane.com>), LastPass (www.lastpass.com) or 1Password (www.1password.com), let you store this encrypted database “in the cloud” and use apps and browser plugins on your devices to access the manager from anywhere. They may also automatically enter your usernames and passwords on webpages and applications for you. You may need to pay a modest fee for these services – Dashlane is free for 50 passwords, \$5/month for unlimited passwords (but also includes breach monitoring to see if any of

your account info has been stolen), and \$10/mo. with added identity protection services; LastPass is free for one user without the ability to share passwords with other users, premium accounts add sharing for \$3/month, family accounts are \$4/month; 1password is \$3/month for one user and \$5/month for family accounts. If you don't want to trust these services (which are very secure) or pay for them, you can use the free and open source KeePassXC (www.keepassxc.org), and can use it across multiple devices by storing it on a cloud drive. Another free alternative is BitWarden (www.bitwarden.com). Free alternatives might not be quite as user-friendly and convenient but will still get the job done securely.

- The EFF has a guide to using KeePassXC available here: <https://ssd.eff.org/en/module/how-use-keepassxc>

Diceware Passwords: You don't need to remember a ridiculous password to have a secure password that you can easily remember. There is another way: diceware passwords. A diceware password uses dice, combined with a list of random words, to generate a truly random and memorable password consisting of a string of words. No worrying about capitalizations, special characters, or numbers. Four random words, either separated by spaces or not, provides a strong password, and six random words is the Fort Knox of passwords... if Fort Knox was more secure. You use dice because humans are very predictable and bad at being truly random. Make your words into a mnemonic or sentence to remember them more easily.

It works like this: roll 5 dice, write down the numbers (in any order) on paper, and find a corresponding word on a diceware word list. Write that word down and repeat three to five times to get your full password. If you don't want to dig up 5 dice, you can use a dice simulator like random.org's (random.org/dice/), but computers aren't as good at being random as real dice. You only need a few of these – one for your password manager and one for each of your devices. For mobile devices, a two- or three-word password is still easy enough to type in quickly and provides exponentially better security than your existing 4- or 6-digit PIN. Here are a few diceware word lists you can use:

- EFF's long word list: https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt
- EFF's short word list (use 4 dice; good for mobile device passwords): https://www.eff.org/files/2016/09/08/eff_short_wordlist_1.txt
- Diceware inventor Arnold G. Reinhold's word list: <http://world.std.com/~reinhold/dicewarewordlist.pdf>

A Warning About Single Sign-Ons:

Many websites today now offer single sign-on access, where you can login to the site using your Facebook, Google, or Amazon username and password. For people who don't use password managers, this is good news – it is less passwords to remember. There are two big downsides:

- 1) If your single sign-on account is compromised, so are all the accounts you use to sign in with it.
- 2) It provides the single sign-on company with information on your outside interests and activities that they can collect and sell.

Instead, use a password manager to create and store your logins with unique, strong, passwords.

One notable exception is Apple's recently introduced "Continue with Apple" feature, which allows you to hide your real email address from the service and requires two factor authentication. Apple says it does not keep records of what services you use or when you use them. Guide available here:

<https://www.macrumors.com/guide/sign-in-with-apple/>

TWO FACTOR AUTHENTICATION (2FA)

Two factor authentication (2FA), which is sometimes called two step verification or multi-factor authentication (MFA), adds an additional layer of security to your accounts by requiring you to provide something you know (your password), as well as something you have (like a code from a device only you have). You have already encountered 2FA without knowing that is what it is. At work, you might have to login to a computer with a smart card and a PIN or use an RSA SecurID token. Your bank might send you an SMS message with a random number to enter. That is all 2FA.

2FA is powerful because even if your password is compromised or guessed, an adversary cannot get into your account without also having access to whatever your second layer of authentication is. Not everything allows for 2FA, but the list of websites grows every day. Most major devices (e.g. Apple, Android, Windows), and popular websites do support 2FA, along with the password managers mentioned above.

There are four flavors of 2FA in common use, **listed from least to most secure**:

- **SMS/Phone Call Verification:** When you login successfully with a password from an unrecognized device, the site sends you an SMS message, or calls you, with a random number code to enter (usually within 10 minutes). This is the least secure because SMS messages are vulnerable to interception by both governments and criminals, but this method still significantly improves security.
- **Email Verification:** Like with SMS verification above, only the code is instead sent to your email. This is slightly more secure because emails are more difficult to intercept, but only if you are using a strong unique password for your email account (most email providers also support 2FA, which you should absolutely enable). For the average person who does not have a strong email password, it is the least secure option.
- **Software Token/Device Verification (recommended, if available):** Software tokens offer a significant improvement over the top two methods because your code *is never sent*. Instead, you install an authentication application on your phone and when you sign up for 2FA on an account, it generates a *shared secret* in the form of a QR code that you scan with your phone's camera (or a string of letters to copy and paste). Using that shared secret, the app generates new six-digit random numbers for each website every 20 seconds. When it comes time to log in, you enter the number for that website from your trusty authenticator app. These software token codes are standardized across websites, so you can use any authentication app that supports them (note: some websites call this method "Google Authenticator," but you can use any software token app of your choice), here are a few: Microsoft Authenticator, LastPass Authenticator, Google Authenticator, or Standard Notes (paid account with TokenVault editor added). Apple uses a variation of this method, where Apple asks you to authorize a login on one of your other Apple devices, which generates a six-digit code to enter.
- **Hardware Tokens:** Hardware tokens, also called security keys, like YubiKey, Thetis FIDO, or the Google Titan Key are the most secure option. You plug them into your device and the presence of the key provides the second layer of authentication. Some also work over Bluetooth for mobile devices. While hardware tokens offer excellent security, few websites support them (but some major ones do, like Google, Dropbox, Microsoft, and Facebook, along with nearly all password managers), and you must carry the key with you to have access to your accounts.

Software tokens provide the best mix of wide availability, ease of use, and security. Get an authentication app like Microsoft Authenticator and start signing up for 2FA for your accounts. LastPass Authenticator, Microsoft Authenticator and Standard Notes allow for encrypted backups of your 2FA tokens to the cloud, a helpful feature (though it is not ideal to keep passwords and tokens in the same place, like with LastPass). [Twofactorauth.org](https://twofactorauth.org) provides a list of websites by category and shows what forms of 2FA they support, as well as links to instructions on how to enable 2FA (under the Docs column). As you are working your way through changing your old passwords, look for 2FA or two-step verification options – many sites only offer SMS verification, but that is better than nothing. If you are using hardware or software tokens for a website, then take the extra step to disable SMS or email verification.

Finally, if you are worried about not having access to your phone in some instances, most sites that allow 2FA also allow you to generate either single use passwords or recovery codes to use instead. You can use these for the times when your phone will not be available, just store them someplace safe (like an encrypted file or database, or on paper in a safe).

A QUICK WORD ON SECURITY QUESTIONS: FALSE ANSWERS

Most websites either offer or require you to provide answers to security questions to allow you to reset your password. The problem with these is that they are often easy to guess. What's worse, people have a bad habit of publishing their answers through Facebook surveys and questionnaires. To combat this, **consider giving false answers**. You can keep these answers in the notes section of your password manager for reference when you need them.

WHILE YOU ARE FIXING BAD PASSWORDS, DELETE OLD ACCOUNTS TO DENY THEM TO THIEVES

As you work your way through changing old passwords, replacing them with complex passwords generated by your password manager, and enabling 2FA for as many accounts as you can, consider deleting old accounts. Most websites give you the option to delete an account, deleting most or all the data associated with it, and most people never do it. Instead, they leave old accounts floating around in databases on the web, ready to be compromised by a thief in a few years. Instead, **if you are not using an account anymore, take the time to delete it**. That will deny the data in that account from a future thief. The previously mentioned websites, deletemydata.io and www.justdeleteme.xyz, are invaluable resources for figuring out how to go about deleting an account, because some sites do make it quite difficult.

CLEAR THE RECORD

When you have completed this Checkup, you should consider going back and cleaning up your online record by opting out from major data providers and data brokers. It is a lot of work, but it will help you start with a cleaner slate, erasing most of what is already out there and available about you. The [Database Removal Checklist](#) will help you get there. These databases will eventually repopulate some of the information you have them delete, but now that your overall data profile is cleaner, it should be a lot less information.

☐ ENCRYPT YOUR DATA AND SECURE YOUR DEVICES

Checkup Actions:

- ☐ Ensure your devices are encrypted using strong passwords, following encryption instructions in attached setup guides:
 - iOS/iPad OS: already encrypted; use a strong alphanumeric diceware password (2-3 words)
 - MacOS: ensure FileVault is enabled and use a strong diceware password
 - Android: ensure disk encryption is enabled and use a strong alphanumeric diceware password (2-3 words)
 - Windows: use either Windows Bitlocker or VeraCrypt to encrypt your full hard drive and use a strong diceware password
- ☐ If you use a cloud storage service like Dropbox or Google Drive, consider switching to a more private alternative like Sync or Tresorit.
- ☐ Ensure auto-update is enabled for all devices and applications.
- ☐ Ensure your Windows PCs are minimally protected with Windows Defender (avoid Kaspersky). Consider a total security suite for all your devices.

ENCRYPT YOUR DEVICES

When combined with strong passwords (above), encrypting your data is the best way to guarantee no one will ever have access to it. While a thief might be able to use your well-encrypted device, they will never gain access to your sensitive information. Encryption is only as good as the password (called a “key”) used to protect it, so make sure you are using a strong password. Store this password in your password manager – if you forget it, you too will be unable to access your data.

Apple iOS/iPadOS devices are encrypted by default using your login PIN or passcode. Late-model MacOS devices are also usually encrypted (you must opt-out of encryption during set up). Most Android devices are also encrypted by default using the same method. Windows devices usually are not. Follow the attached guides to ensure your devices are encrypted.

If your hard drive is encrypted, then you don’t need to worry as much about securely deleting files, but you should know that files are not deleted when you delete them. A secure deletion tool like Eraser (eraser.heidi.ie) or Bleachbit (www.bleachbit.org) will ensure your deleted files truly cannot be recovered, even if someone gains access to your encrypted drive.⁵ Bleachbit also helpfully cleans and removes other records and logs for an extensive list of applications.

⁵ This is not completely true for solid state drives (SSDs), which is what most new devices come with. As with all drives, your best defense is full disk encryption. When you are done using an SSD, you can securely erase it with a tool like Parted Magic (www.partedmagic.com).

PRIVATE CLOUD STORAGE ALTERNATIVES

Cloud storage is extremely popular, and for good reason: it is convenient. You can store your files in the cloud and access them anywhere, and services like Dropbox make it seamless. The catch is that most cloud storage providers are not private. There are many popular cloud storage providers: Dropbox, Google Drive, Apple iCloud⁶, Microsoft OneDrive, and Amazon Web Services to name a few. While they all talk about the robust encryption they employ, they mostly overlook the detail that they hold the keys to that encryption, not you. They have full access to your files and what you are storing. They can read, analyze, and sell information on your storage habits (privacy policies also vary considerably; iCloud is the most private of those mentioned).

While the most secure choice is to avoid cloud storage, there are more private options available with good security. Look for options with end-to-end encryption.⁷ Sync (sync.com) is a great Dropbox replacement with similar functionality but promises “zero knowledge” – Sync encrypts your files with encryption keys you control – Sync does not know what you are storing on its servers. Tresorit (tresorit.com) is another alternative with similar security and functionality. Both support 2FA.

Advanced users may consider hosting their own cloud storage with ownCloud (owncloud.org) or NextCloud (nextcloud.com).

PROTECT FROM INTRUSIONS: AUTO-UPDATE AND ANTIVIRUS

Update your operating systems and applications regularly and always enable auto-update. The most common way for hackers to gain access to your devices and data is through known exploits that software developers have already patched. If you regularly update everything, you are safe from most of those attacks. The attached device guides provide instructions on how to ensure auto-updates are enabled.

The second part of a good defense is good antivirus software. This is particularly important on Windows computers. Microsoft’s Windows Defender, included with Windows, is sufficient when enabled. Antivirus is also a good idea for Android devices because many no longer receive software updates. If you don’t trust yourself to make good decisions about suspicious links or phishing attacks (which can be very targeted and sophisticated), a security suite is a worthwhile investment. Options include Bitdefender Total Security, McAfee Total Protection, Norton 360 Deluxe, or Webroot Secure AnyWhere Internet Security Complete. In 2019, the U.S. Government permanently banned government agencies from using Russia-based Kaspersky Lab products over its relationship with Russian intelligence services; you should heed the warning, play it safe, and **avoid Kaspersky products**. **An antivirus program has deep access to your device and files, so you need to completely trust the company behind the program.**

⁶ Apple is reportedly working on adding end-to-end encryption for iCloud but has not implemented it yet. **Some specific iCloud services are end-to-end encrypted:** Apple Card transactions (iOS 12.4 or later), Home data, Health data (iOS 12 or later); iCloud Keychain; Maps favorites, collections and search history (iOS 13 or later); memoj (iOS 12.1 or later); payment information; QuickType keyboard learned vocabulary (requires iOS 11 or later); Safari history and iCloud tabs (iOS 13 or later); screen time; Siri information; Wi-Fi passwords; W1 and H1 Bluetooth keys (iOS 13 or later).

⁷ **End-to-End Encryption:** You will see this term a few times. In the simplest terms, if something is truly end-to-end encrypted, it means that only you (and your recipient in the case of messages/emails) can read/access the information. The information is encrypted such that *the service does not have keys to access it*. It is garbled nonsense to everyone but you.

☐ COMMUNICATE SECURELY WITHOUT BEING MONITORED

Checkup Actions:

- ☐ Use an encrypted DNS service (e.g. Cloudflare 1.1.1.1), see browser configuration guides for [Firefox](#) and [Brave](#).
- ☐ Acquire, download, and use a paid, privacy-oriented, VPN service, especially on a public network (or use Cloudflare WARP).
- ☐ Switch to [Signal Messenger](#) for a more secure alternative than traditional phone calls and SMS messages.
- ☐ Enable Wi-Fi calling on your cell phones if it is part of your cell phone plan.

ENCRYPT YOUR DNS REQUESTS

DNS requests are your devices' requests to visit websites – a DNS server takes the human-friendly “www.” version of what you are trying to visit and translates it into a computer-friendly IP address (e.g. google.com is actually 8.8.8.8). DNS requests can reveal your browsing activity unless they are encrypted. DNS encryption is new, and not widely available. Cloudflare is a privacy-oriented free DNS provider that supports encrypted DNS. The attached [iOS](#) and [Android](#) guides provide instructions for installing Cloudflare's 1.1.1.1 app, which easily enables DNS encryption. Android users with Android 9 or later can also enable encrypted DNS in settings if you don't want to download the app (see guide). The [Firefox](#) and [Brave](#) guides also provide instructions on enabling encrypted DNS.

VPNS: ENCRYPT YOUR BROWSING

A VPN (virtual private network) creates an encrypted channel between your device and the VPN service. You might have to use a VPN for work to connect to your organization's network – it is a secure, remote method for connecting to another server. It is also a terrific way to prevent your internet service provider from tracking and selling information on your internet activity. A VPN conceals your IP address from sites you visit, and lets you spoof your browsing location by choosing a server from another region (see [Know Your Rights](#) section above). You should always use a VPN when connecting to an unsecured or public network, such as in a hotel, airport, or coffee shop, because a VPN prevents both the network owner and other people using the network from

Cloudflare's WARP Service

Privacy-oriented cloud infrastructure provider Cloudflare pairs a service called WARP with its 1.1.1.1 encrypted DNS app. Cloudflare markets WARP as a modern VPN.

Like a VPN, WARP establishes an encrypted connection with Cloudflare's servers, encrypting your traffic from snooping by public networks or your service provider. You may even see faster speeds with WARP, because it uses modern VPN protocols (WireGuard) and Cloudflare's infrastructure is so fast. **And it is free.**

Cloudflare also offers a WARP+ service for \$5/month that uses Cloudflare's high-speed private Argo network to route your encrypted traffic, avoiding the crowded public spaces of the internet, providing speed boosts of up to 30%.

However, unlike a normal VPN, it does not conceal your IP address from the sites you visit and does not allow you to change regions/locations by switching servers.

For most people, WARP is a great “switch and forget” option to more private browsing.

snooping on you. A VPN also prevents most potential man-in-the-middle attacks, where an adversary pretends to be a Wi-Fi network you want to connect to in order to snoop on your traffic (e.g. HHonors, Starbucks, etc.). But even at home or on cellular networks, a VPN keeps your service provider from tracking your internet activity.

You can use a VPN without experiencing much of an impact on your internet browsing. Websites might ask you more often to prove you are not a robot, and you may run into trouble using region-specific services like Netflix or YouTube. A VPN will typically decrease your internet speed, but you won't notice a difference if you are using a high-quality paid VPN (none of these downsides apply to Cloudflare's WARP, discussed in the tone box).

Not all VPN providers are equal. Most free VPNs provide you with no improvement in security or privacy – they log, track, and sell information on your activity.⁸ Even many paid VPNs still log activity, potentially providing it to law enforcement authorities or thieves who wish to steal it (especially foreign governments). **You want a paid VPN service that has a strong reputation for privacy and minimal logging.** Some good options include: NordVPN (nordvpn.com), Private Internet Access (privateinternetaccess.com), or ProtonVPN (protonvpn.com, also offers a solid free alternative, see footnote below). Service typically costs 3-8 dollars/month.

Using these services is straight forward – download the application for your device, log in, and turn it on. For most uses, you want the closest/fastest server, but you can make it seem like you are browsing from a different region or country by using servers in those locations.

SECURE YOUR COMMUNICATIONS WITH SIGNAL MESSENGER

Traditional phone calls and SMS messages should always be your last choice, they are neither private nor secure. Common encrypted messaging applications allow you to communicate securely by supplying end-to-end encryption for your messages and calls. While there are many such services (Viber, WhatsApp, etc.), **this Checkup strongly recommends Signal Messenger** (www.signal.org), developed by the privacy non-profit Signal Foundation, for its strong commitment to privacy and security, ease of use, and robust features (including voice/video calling). Unlike many other services, Signal collects almost no information on you and your activity, and more importantly, cannot collect it. Every aspect of the service is end-to-end encrypted and not visible to Signal or its servers: your messages, calls, information about who you are communicating with and when, your profile information, and even if you use GIFs or stickers in messages – all end-to-end encrypted. Signal only ever knows three things about you: your phone number (but not your name), the date you registered, and the last day your account was active. It has no information on who communicate with, when, or what you communicate.

The attached guide provides instructions on downloading and getting started with Signal. Signal is growing in popularity, but you may need to recruit your friends and family to come along. You can invite them to join from the Signal app.

Another private and very secure alternative is Wickr Me.

If you cannot get people to use Signal, **good popular alternatives are Apple's iMessage (messages) and Facetime (voice/video calls) services**. While only available for Apple devices, iMessage and Facetime are end-to-end encrypted and private – Apple keeps some information on your calls, but only for 30 days, and no one can

⁸ ProtonVPN is a notable exception to this rule. It is very private and offers a free option with lower speeds/bandwidth from the paid version. If you only need a VPN occasionally for casual browsing, this is a great private and secure option.

read your messages or listen to your calls. However, only blue iMessages between Apple users are secure – green messages are unsecure SMS messages.

While much more secure than a traditional phone call or SMS message, services like Viber, WhatsApp, Skype, Snapchat, or Facebook Messenger are not private because they collect and sell/share a lot of information on your contacts and communications.

WI-FI CALLING

Most cell phone providers now offer Wi-Fi calling, which lets you use Wi-Fi networks to make calls instead of using the cellular network. When combined with some changes in your phone's settings, this provides your cellular company with slightly less information on your phone calls. It also may make your calls more difficult for an adversary to intercept. Wi-Fi calling is not a huge gain for privacy, but it is something worth enabling if your cell plan allows for it. See configuration guides for instructions.

When traveling, especially to high-risk countries, Wi-Fi calling does significantly improve your privacy because your calls don't go through a foreign cellular provider's network; they are sent over an encrypted channel directly to your home cell phone provider.

☐ SECURE YOUR HOME NETWORK

Checkup Actions:

- ☐ Secure your home router:
 - ☐ Consider replacing a router provided by your service provider with one you own.
 - ☐ Set a strong password on your home network router.
 - ☐ Ensure your home router's firmware is up-to-date, and if available, set it to auto-update.
 - ☐ Set your home router to deny external/remote administration or configuration; disable UPnP.
 - ☐ Ensure your home Wi-Fi network is secured using WPA2 encryption (WEP and WPA are easily cracked) and uses a strong password.
- ☐ Change default passwords for any other device (e.g. cameras) connected to your network and ensure they are up to date.
- ☐ If you have a secure Wi-Fi guest network, segregate internet-of-things devices onto your guest network (e.g. cloud cameras, digital assistants).

SECURING YOUR HOME ROUTER

Your home router is your first and primary line of defense. Your router protects and conceals the devices behind it from would-be attackers. **Your security is only as good as your router's.** Configuring a router varies by make and model, so you will need to consult your router's manual. If you don't have it, search the manufacturer's website for the model of router that you have. If you don't know what a router is – it's the device that sits with and is connected to your modem (which connects to the outside with a coax or fiber optic cable, or a phone line) and provides your home with its network (usually with Wi-Fi). Some homes use combined modem/routers, often supplied by your internet service provider. You may still be able to configure a router provided by your service provider, but you should consider replacing it with a router you own and have full control over for maximum security.

You want to do a few things to your router to ensure it is secure. First, ensure you are not using the default password and set a strong password (you can use your [password manager](#)). Second, ensure its firmware is up-to-date, and see if you can enable it to auto-update (it may give you gloom and doom messages about losing its configuration, that never actually happens). **Make sure to disable any feature that allows remote administration or configuration.** If available to disable, disable universal plug-in-play (UPnP), which hackers can use as an open door to attack devices on your network (this may affect usability of some devices). Finally, ensure your home Wi-Fi network is secured with WPA2 encryption (or WPA3 if available), hackers can easily circumvent older encryption schemes like WEP or WPA. Use a strong [diceware password](#) to encrypt your wireless network and store it in your password manager – this will make it easy to type in when you need to. You can also hide your Wi-Fi network, which is a good idea, but does little (anyone can still easily see its name with free software, and it will still likely be [surveyed by nearby devices](#)).

SECURE OTHER DEVICES ON YOUR NETWORK

You want to ensure any device connected to your network is also secure. Hackers often hijack devices like cameras to spy inside peoples' homes or have used them to conduct large-scale attacks against public networks. They can do this because many people never change the default passwords.

It is imperative that you check to ensure every device on your network has up-to-date software and that, if possible, you have changed the default password on the device to a strong password stored in your password manager. With internet-of-things and smart-home devices, this can include a wide range of devices: cameras, TVs, thermostats, DVD players, stereo receivers, robotic vacuum cleaners, smart home assistants (e.g. Amazon echo), washer/dryers, refrigerators, dishwashers, security systems, locks, and smart lights. Many of these devices won't allow you to change or set a default password and instead use your service account password to protect them, so make sure that your account password is strong and enable 2FA when available. If you are up to the challenge, you should also try to isolate these devices onto a separate network. If you have a secured guest Wi-Fi network at home, then an uncomplicated way to isolate these devices is to put them all on the guest Wi-Fi network, which will keep them from being able to collect information on or access your primary devices.