

☐ CHOOSE PRIVACY-ORIENTED ALTERNATIVES

Checkup Actions:

- ☐ Consider changing the services you use to private alternatives.
- ☐ Be careful about the devices you buy and services you use and avoid devices and services from Chinese companies.

PRIVATE ALTERNATIVES

The services you use can be a major source of data collection. As discussed in Part I, popular service providers for things like email (Gmail, Yahoo Mail, Outlook.com, etc.) and cloud storage are a major source of information for companies to accumulate about you and sell/share, including doing things like scanning your emails to track your purchases. This guide has already mentioned some of these but it is a crucial point to reinforce – you don't have to use services that don't respect your privacy. They may be free, but they are making money off your data. Here are some alternatives:

- **Email:** **ProtonMail** (protonmail.com), **Tutanota** (tutanota.com), **Posteo** (posteo.de), **Mailfence** (mailfence.com), **Mailbox.org** (mailbox.org), or **StartMail** (startmail.com). Unlike the popular services mentioned above, these email services will not read your emails, analyze your contacts and who you are communicating with, or sell your information, and they keep minimal logs. They all enable you to send encrypted emails if the recipient's email supports it (using OpenPGP). ProtonMail and Tutanota offer superior encryption to PGP for messages to other users within those services (so recruit your friends). Paid ProtonMail and Tutanota accounts allow you to send an encrypted email to anyone, but you must pass them a password separately.
- **Cloud Storage:** **Sync** (sync.com), or **Tresorit** (tresorit.com). Discussed above.
- **Calls/Messaging:** **Signal Messenger**, or when unavailable, **Apple iMessage/Facetime**. Discussed above.
- **Browser:** **Firefox** (mozilla.org) or **Brave** (brave.com). Discussed above.
- **Documents/Spreadsheets:** Use a desktop-based application like Microsoft Office (which does collect some data by default, check the settings), or LibreOffice (better). Or for cloud-based editing (instead of Google Docs), **CryptPad** (cryptpad.fr), **Cryptee** (crypt.ee), or **Standard Notes** (standardnotes.org). Cryptee is also a practical alternative to Google Photos. Standard Notes offers spreadsheet and rich document editing with paid accounts.
- **Cloud Notes:** **Standard Notes** or **Joplin** (joplinapp.org). Both offer end-to-end encryption (must be enabled) and can sync across devices. Joplin can import from Evernote. As previously discussed, paid Standard Notes accounts offer more – rich text documents and spreadsheets and a 2FA token manager that you can securely access from any of your devices.
- **Maps:** **OsmAnd** (osmand.net) offers offline maps and navigation so you don't have to provide location information to a service like Google Maps or Waze. While it will build routes based on traffic profiles, it does not yet supply real-time traffic information. For Apple Devices, **Apple Maps** is a surprisingly private alternative (and has improved enormously since its troubled launch). With Apple Maps, your device encrypts and stores all location histories, searches, parking spots and collections locally on your phone, and if backed up to iCloud, this information is end-to-end encrypted so Apple cannot see it. Apple does

collect some data on your use to improve traffic analysis, which Apple says it anonymizes with random, continuously changing, identifiers – you can, and should, disable this collection (see attached guides).

A useful resource for recommendations on privacy-oriented services is privacytools.io.

In the area of financial data and payments, there are few good options. Apple, again, supplies the best mainstream choices. Apple's credit card, Apple Card, and to a lesser extent, Apple Pay, is the first and only attempt from a major company at a private version of electronic payments. Apple collects no information on Apple Card transactions (who you buy from, when, or how much) besides some anonymized analytics data (the fact you have an Apple card and how often it's used), which you can opt-out of through an email to Apple (read the privacy policy for instructions). Your device stores your digital card in its ultra-safe Secure Enclave (where your device also stores your biometric information). Goldman Sachs, the card issuer, also gets much less data on you than with traditional credit cards and is bound by a strict privacy policy that forbids it from sharing or selling the data it collects. With any Apple Pay transaction, vendors do not receive your credit card information, limiting their ability to share it and track you across stores. All Apple Pay information is either stored locally on your devices or end-to-end encrypted so that Apple cannot see or collect it.

Another possibility is Albine Blur (albine.com), which for \$100/year provides a service that allows you to generate virtual credit card numbers for online use with any of your credit cards; the service also supplies email aliases and virtual phone numbers (see [advanced techniques](#), below). A virtual credit card number is just a generated credit card number that masks your real credit card information from the vendor. You can set custom limits for virtual cards or make them one-time-use to prevent theft. Together with the tools Blur provides, you can shop online without supplying anyone your real credit card number, email address, or phone number. The U.S.-based company's privacy policy is also clear and solid – Albine says it will not share your information with anyone without a warrant.

DEVICE SELECTION

For most users not willing to go the extra mile for security and privacy, or lacking the technical skills to get there, Apple products offer superior privacy and security over available alternatives. In general, Apple devices have better out-of-the-box security design than Windows and Android counterparts, and Apple has staked its reputation on privacy, offering default privacy features like encryption at rest, end-to-end encryption on iMessage/Facetime, and warnings about when applications are collecting your location information. Apple devices still collect a fair amount of information by default but offer good configuration options to reduce it. Most of the information stays on your device, and some of the more sensitive features backed up to iCloud are end-to-end encrypted so that Apple cannot read the data (see footnote in cloud storage section, [here](#)). Overall, Apple seems genuinely committed to improving privacy while balancing ease-of-use but does collect some data when not disabled.

With the introduction of Windows 10, any mirage that Microsoft was interested in privacy disappeared. Default installations of Windows 10 collect a lot of information – location, usage and activity, Wi-Fi and Bluetooth information, application usage, internet browsing, and more. Various optional features press for more information, like contacts, phone numbers, and access to SMS messages. Most of this collected information goes off to Microsoft's servers. Overall security design has improved with each updated version of Windows, but Windows still lags its competitors in this department.

Android devices suffer from a couple of major problems. Importantly, as discussed earlier, most Android devices are ineligible for updates to protect them from critical security flaws. In March 2020, British consumer watchdog Which? estimated there are 1 billion active Android devices no longer able to receive security updates. That is

troublesome. On the privacy front, a 2018 Vanderbilt [study](#) found that **Android devices, on average, collected ten times more data than their Apple counterparts, sending it all off to Google servers.**

For users willing to try out Linux distributions, or explore custom ROMs for Android, there are more secure and private alternatives than Apple, but they also come with their own dangers (particularly the ROMs). Linux is a great, very private choice for those willing to take the plunge. Modern Linux distributions like Linux Mint or Ubuntu allow an easy transition for Windows users. For advanced Linux users, Arch Linux allows extreme customization, and QubesOS provides vault-like security.

A WARNING ABOUT CHINA: AVOID CHINESE COMPANIES AND SERVICES (AND RUSSIAN TOO)

Modern China is a sophisticated, technology-enabled, surveillance state. China stands for the opposite of privacy and personal security, and China's proliferation and export of advanced surveillance capabilities, such as in the form of so-called "safe cities" capabilities, makes it a threat to privacy everywhere, including in cities in the U.S. and Europe. More concerning, **China's 2017 Internet Security Law requires Chinese companies supply any information they collect to the Chinese Government and security services – that's not just information from within China's borders.** The Chinese government may also force Chinese companies to undermine security and implement backdoors in their products to enable collection. Consequently, you should completely avoid buying devices from Chinese brands and using services from Chinese companies. Specifically, you should avoid services like WeChat, Weibo, and TikTok. Russia presents a similar threat to privacy, so it's safest to also avoid services from Russian companies like Kaspersky Lab ([discussed above](#)), Telegram⁹, Vkontakte/Vk, or Yandex. Here is a list of popular Chinese device manufacturers to avoid:

Avoid: Chinese Brands

BLU	OnePlus	Xiaomi (Mi)
Hisense	Oppo	ZTE
Huawei	TCL	
Lenovo	Vivo	

PRIVACY HAVENS

Many privacy experts also advocate you avoid using services based in countries with poor privacy laws, including the U.S., and avoid services hosted in countries who are close allies of the U.S. if you are concerned about U.S. Government surveillance. Regardless of whether you are concerned with such things, it's undeniable that some countries offer rock solid privacy laws that make it much more difficult for a government to lawfully obtain your data (e.g. through a warrant), and also significantly restrict or ban companies' ability to lawfully collect and share/sell data on you. The following are some privacy havens:

Czech Republic	Germany	Ireland	Panama	Sweden
Denmark	Iceland ¹⁰	Malta	Seychelles	Switzerland

⁹ Following trouble with the Russian government, Telegram's development team recently moved to Dubai. While touted by some in the privacy community, the service leaves much to be concerned about – end-to-end encryption is closed source and not enabled by default, and messages, contacts, and profiles are stored on Telegram's servers.

¹⁰ Iceland is sometimes called the "Switzerland of data" for its very rigid data privacy laws.

☐ OTHER SECURITY PRACTICES

Checkup Actions:

- ☐ **Get in the habit of turning off Bluetooth and Wi-Fi when you are not using them.**
- ☐ **Don't plug your devices directly into public USB ports to charge them without a data blocker.**

STOP BLUETOOTH AND WI-FI TRACKING

As previously discussed, other devices, including other people's phones, collect information automatically broadcast by your devices when you have Bluetooth and Wi-Fi turned on. Data aggregators and others who get it can use this information to track you. **The simple solution is to turn off Bluetooth and Wi-Fi when you are not using them.** If you don't routinely use Bluetooth, just keep it off all the time. You should be aware that this applies to any Bluetooth device, including any wearable Bluetooth devices, like smart watches, fitness trackers, or headphones – advertisers and adversaries can all track you this way, and you might not be able to turn off these devices' ability to transmit. If you cannot stop some Bluetooth devices from transmitting, leave them at home if you don't want to be tracked.

You should also forget/delete public Wi-Fi networks from your Wi-Fi settings after you use them.

DON'T PLUG YOUR DEVICES DIRECTLY INTO PUBLIC USB CHARGING PORTS

Here is the scenario. You are traveling, or in a local coffee shop, and have some time to kill. You see a USB port on the wall and plug your phone in to charge. As it is charging, you unlock it and go about your business of surfing the net, answering emails, etc.

Meanwhile, an adversary could have downloaded every ounce of data on your phone after you unlocked it (which decrypts the data and makes it available for download). Typically, criminals have hijacked these public terminals, or governments if you are in an authoritarian country (known as "juice jacking"). Adversaries can use this method to deliver a trojan to your device to allow long-term compromise of your data. It is not just criminals and governments – the company itself may pull data from your device to collect information on you as a consumer (particularly in an airplane).

There is a cheap and simple fix: a data blocker. You can get a data blocker for \$5-10 on Amazon and comparable sites. It is a small, simple device that looks like a flash drive – all you do is plug your USB charging cord into it, and the data blocker into the public port. It lets you charge your device but will not allow data to transfer.

☐ SPREAD THE WORD, YOUR PRIVACY IS COUNTING ON IT

Checkup Action:

- ☐ Discuss and share this guide with your friends, family, and coworkers. If you are savvy, offer to help them with some of the more difficult actions.

Privacy is about more than just you. Your friends, family, and coworkers are continually collecting and sharing data about you. They take and share pictures. Email and talk on the phone about you. Talk about you on social media. Even total strangers unknowingly collect information on you with their devices (e.g. Bluetooth and Wi-Fi beacons) that is collected and sold around the world. Let's face it – most people have not done the work to make their data – your data – more private. The best thing you can do is pass this guide along to them, and convince them to change, for both your sake and theirs.

☐ GET YOUR ANNUAL CHECKUP

Checkup Actions:

- ☐ Set a calendar reminder to review social media settings every 3 months.
- ☐ Set a calendar reminder to conduct an annual checkup:
 - ☐ Review your password manager for accounts you no longer use and close/delete them to protect your data from breaches.
 - ☐ Change passwords
 - ☐ Revisit privacy settings and options for your devices and services you use.

GET STARTED ON

THE COMPLETE CHECKLIST NOW

Now that you understand the challenge and what you can do about it, it's time to dig into the checklist. If you want to complete the full Checkup, it's best to use the attached Complete Privacy Checkup Checklist. It's organized in the most efficient order to accomplish all of the Checkup items, whereas they are organized by topic here.

SOME ADVANCED TECHNIQUES

This section briefly discusses some more advanced privacy techniques. Some of these are approachable for the average person (e.g. virtual phone numbers), but others could put you more at risk if you don't know what you are doing (custom Android ROMs).

VIRTUAL PHONE NUMBERS (DIFFICULTY: EASY)

Don't like giving out your phone number to companies or to strangers on Craigslist? Virtual phone number services let you give out alternative, "burner," numbers that can still receive phone calls and often SMS messages. There are plenty of options for virtual phone numbers. Google Voice allows you to create virtual phone numbers that can receive texts for free, but it comes at the cost of Google knowing everything about who you are calling and when. You might find that an acceptable compromise for hiding your regular phone number from whoever you are calling or giving it to. There are also several apps that offer paid, but affordable, options: Burner, Vumber, Tossable Digits, Second Phone Number, and Talkroute are a few.

EMAIL ALIASES (DIFFICULTY: EASY)

Like virtual phone numbers, many email providers offer email aliases as part of your account. You log into your one email account but can generate aliases to provide to companies and services. In an ideal scenario, no two companies have the same email for you, but even with just a few aliases, you can easily segregate services and keep companies from having the email address you use to communicate with friends. You can also easily turn an alias off – shutting down spammers using it to send you messages. Some services, including Gmail, offer a lesser version of this, where you can make an alias by adding the + operator to your normal email address (for example, johnsmith@gmail.com can tell Amazon his email address is johnsmith+amazon@gmail.com). There is no limit to how many of these you can create, but unfortunately their utility is limited. The companies themselves know this trick and strip the + operator from your email when sharing it with advertisers and other companies. For sites that use your email address as a login, it does supply some added security by giving you a unique username for that site. As discussed in the tone box in the section on [hardening your accounts](#), Apple's "Continue with Apple" single sign-on service can also generate email aliases.

BOOTABLE LINUX OR VIRTUAL MACHINES (DIFFICULTY: MEDIUM)

A bootable Linux thumb drive or "live CD" can be a powerful privacy tool. You can download any Linux distribution of your choice for free, use a tool like Rufus to put it on a thumb drive (or CD if the distribution is small enough), and boot into your own private, one-time use, computer. When you restart again, everything you did on your bootable Linux operating system is gone forever – lost with the electrons in your RAM. It also allows you to change your digital signature quickly and easily. Any Linux distro will do, but the Department of Defense's Trusted End Node Security (TENS) is purpose-built for the task.

Like a bootable thumb drive, you can also run a Linux virtual machine (VM) within your existing operating system for free using VirtualBox. You can "clone" these VMs and destroy them when you are done with them, setting up a

new clone with different identifiers. If you really want to get sophisticated, you can pay to host a VM in the cloud using a cloud hosting service. If you use that cloud VM for your browsing and connect to it through a VPN service, then it would be extremely difficult to link it to you.

TOR (DIFFICULTY: EASY, BUT POTENTIALLY DANGEROUS FOR A NOVICE)

Tor, sometimes called an “onion router,” is a network of private servers that use a shared protocol to route encrypted traffic through multiple servers before exiting to the web. Tor effectively anonymizes your traffic. Tor is most often what people are talking about when they talk about the “dark web.” It is super simple to use – just download the Tor Browser (tor-browser.en.softonic.com) and use it. It will anonymize your activity, but **there are some serious downsides for novice users**. First, Tor is the wild west, and if you don’t know what you are doing you can easily expose yourself to attackers. Second, you should avoid any activity when using Tor that connects your activity to your identity, such as logging into a website. **Third, the Tor exit nodes – the servers your traffic leaves to visit the internet – are under close surveillance by good and bad actors alike (both independent hackers/criminals, governments, and security researchers)**. This can make you a target. Fourth, it’s slow. Fifth and finally, your internet service provider will know you are using Tor, which could draw more scrutiny to you. You can prevent that by combining it with a VPN, but that combination can also increase your “attack surface” – leaving your traffic more vulnerable overall to adversaries.

ENCRYPT ANY EMAIL WITH PGP (DIFFICULTY: MEDIUM)

You can stick with Gmail if you want to, and still encrypt it with PGP. PGP uses what is known as public key cryptography to encrypt emails. Very simply, with public key encryption, you have two keys – a private key that you keep secret, and a public key you provide to others. In practical terms, this means to send and receive an encrypted email three things need to happen: (1) You have your private key, (2) Your recipient has your public key, and (3) You have your recipient’s public key. **Importantly, you must exchange public keys with your recipient before you can communicate**. It is the key exchange that can make this a bit difficult, since it involves multiple steps to export, send, and import keys. Once you exchange keys, it’s simple.

You have a few options to do this. You can use a key manager like GPG4Win/Kleopatra (gpg4win.org), which will let you store, import, and export your private key, public key, and the public keys of your contacts. The EFF’s Surveillance Self Defense guide has guides on how to use the Thunderbird email client and Enigmail key manager to send/receive PGP encrypted emails (ssd.eff.org). You can also use a key management browser extension on the desktop, like Mailvelope or Flowcrypt (for Gmail). Finally, if you are willing to change email services, you can use one of the email services discussed in the Private Alternatives section, which offer integrated key management.

PRIVATIZE YOUR ANDROID DEVICE WITH A CUSTOM ROM (DIFFICULTY: HARD AND DANGEROUS)

As previously discussed, Android devices have some serious problems, not least of which are their tight integration with Google, a company not particularly interested in your privacy. Advanced users have the option of ditching Google in favor of a custom, more private, ROM like Lineage OS, CopperheadOS, Paranoid Android, GrapheneOS or eFoundation. This requires you to replace your device's firmware – its core functionality software – with a custom version.

The result can be superior security and privacy compared to both stock Android and Apple operating systems, but there are significant pitfalls. First, it can be difficult to get to work correctly and has a small chance of permanently disabling your device. Second, it can be dangerous – you need to completely trust the software you are installing on your device because it can control it completely. While these ROMs are open source, the code base is complex, and there is room for error – either an unintentional security flaw or intentionally added vulnerabilities to exploit devices. Third, if you want privacy you will also have to abandon the Google Play store in favor of something like F-Droid, or directly “side-loading” applications. While this means you are no longer married to Google, it also means you can potentially open your device to untested and unsecure applications.

Managed properly by a savvy user, a custom ROM can be a marked improvement in security and privacy, but it's dangerous territory to venture into for most people.

Part III: Exercise Extra Caution When Traveling

You are at higher risk when traveling, period. In an unfamiliar environment, you are a bigger target for criminals of all kinds, and when crossing borders, you are much more likely to be under government scrutiny by customs, law enforcement, and intelligence officials. This section has two parts – general data security and privacy tips for traveling, and more thorough recommendations for traveling to high-risk countries (especially China and Russia, but the list is long).

ROUTINE TRAVEL

When you are traveling domestically, or to minimal risk countries (e.g. Europe), you should still step up your security game. Depending on who you are and what your business is, you may want to follow the tips in the high-risk section even when traveling to minimal risk countries.

KEEP CONTROL OVER YOUR DEVICES

When you are traveling, keep physical control over your devices, especially in transit. Keep them in carryon bags or on your person; never check them. On the plane, keep tablets and laptops under the seat in front of you – not in the overhead bin. Any time spent away from your devices is an opportunity for adversaries to steal, tamper with, or copy them.

Hotels can be particularly tricky. If you can keep your devices on you, do it. Hotel staff – and government officials – can access hotel safes while you are out of your room. Safes are better than nothing, but don't consider them completely secure (especially in high-risk countries).

ENSURE DEVICES ARE ENCRYPTED AND TURNED OFF WHEN NOT IN USE

If you encrypted your devices (see attached guides for your devices), then when you turn them off your data is completely safe – even from a sophisticated government intruder if you used a strong password. Keep your devices turned off when not in use, **and especially when crossing borders/going through customs**. For domestic travel, keep them locked when not in use is sufficient.

KEEP WI-FI AND BLUETOOTH OFF WHEN NOT IN USE; CONSIDER DISABLING CELLULAR

This tip was discussed above, but it is particularly important to keep Wi-Fi and Bluetooth turned off when traveling because attackers looking to target your devices, particularly through Wi-Fi man-in-the-middle attacks, prowl airports and hotels. If you are concerned about government surveillance where you are traveling, also consider turning off your cellular antenna when you don't need it.

SERIOUSLY: DON'T PLUG YOUR DEVICES INTO PUBLIC USB PORTS

Previously discussed, but especially important when traveling. Get and use a data blocker.

GET AND USE A TRAVEL WI-FI ROUTER

A travel Wi-Fi router is just that – a small portable router that broadcasts a private Wi-Fi network for your devices. They come in two flavors: cellular and non-cellular (also called a portable Wi-Fi bridge). Cellular travel routers receive an internet connection over cellular data service and broadcast a Wi-Fi network for you. Non-cellular routers take a public network (Wi-Fi or ethernet), like a hotel's Wi-Fi, and make a private network just for you. If you secure the router properly (discussed in Part II, above), you will be hiding your devices behind a secure barrier. The public networks will not be able to see or collect information on your devices, and adversaries won't be able to target them without considerable effort.

You can configure some travel routers to push all your traffic through a VPN, an excellent feature because you should always use a VPN when traveling...

ALWAYS USE A VPN

When you are on a public network, use a VPN or Cloudflare's WARP always ([discussion here](#)), even when using a travel router. This will keep your internet traffic safe from prying eyes.

BEWARE OF RENTAL CARS

As discussed in part I, cars are major data collectors, and rental car companies have increasingly upgraded sensors to collect more data. Don't connect your devices to a rental car (USB or Bluetooth) – the car will syphon up as much of your data as it can (contacts, messages, and more). Criminals or governments can use this connection to deliver a trojan horse to your device to gain persistent access to it long after you leave.

If you feel you absolutely must connect your device to a rental car, the app Privacy4Cars supplies detailed instructions on how to remove some of your data before you turn the car back in.

TRAVEL TO HIGH-RISK COUNTRIES: YOUR DATA IS AT EXTREME RISK

Traveling with your data to high-risk countries is a very risky proposition. These are countries with law enforcement and intelligence services that have few, if any, restrictions, and either have developed sophisticated data collection capabilities, or bought them from surveillance exporters like China. Others have very sophisticated criminal networks that may target you. A few things to know up front:

- 1) Government or criminal adversaries will likely collect/steal information you take to, or access in, these countries.
- 2) These adversaries will likely fully exploit any devices you take and may persistently compromise them – reporting data back to the country long after you leave.
- 3) Your security practices are not better than their capabilities.
- 4) They do not require physical access to your devices. They can remotely exploit your devices – you are on their networks, in their territory, and they have hundreds of ways to gain access to your devices and accounts.

Recommendations in this section are heavily derived from two excellent sources:

- 1) Stanford University's recommendations to its staff for travel to high-risk countries (and list of high-risk countries): <https://uit.stanford.edu/security/travel/high-risk-countries-recommendations>
- 2) University of Rhode Island's guidance for travel to China or Russia: <https://security.uri.edu/travel/travel-to-china-or-russia/>

HIGH-RISK COUNTRIES

The following are countries/areas where your data are at particularly high-risk. **Countries in bold** are those with sophisticated electronic surveillance capabilities – nearly everyone should follow the best security practice for these countries. Among these, China, Russia, and Israel are the most dangerous to your data.

Afghanistan	Haiti	Pakistan
Algeria	Honduras	Philippines
Belarus	Iran	Russia
Burundi	Iraq	Saudi Arabia
Cameroon	Israel	Somalia
Central African Republic	Kenya	South Sudan, Republic of
Chad	Lebanon	Sudan
China (including Hong Kong)	Libya	Syria
Colombia	Mali	Thailand
Congo (DRC)	Mauritania	Turkey
Crimea (Region of Ukraine)	Mexico	Ukraine
Cuba	Myanmar	Venezuela
Egypt	Niger	Yemen
El Salvador	Nigeria	Zimbabwe
Eritrea	North Korea	

HIGH-RISK TRAVELERS

Some groups of people are at higher risk from data threats when traveling and this guide strongly recommends high-risk travelers follow the below best/highest security option for all travel to high-risk countries. This is critically important if you are also traveling to one of the countries listed in bold, above. The following categories of people are at especially high-risk of data threats when traveling:

academics/researchers	engineers/scientists	nationals or ethnic nationals of
businesspeople ¹¹	military, government officials	the visited country ¹²
clergy and missionaries	and contractors	NGO/non-profit workers
	journalists	

Even if you don't fall into these groups, if you are associated with someone in one of these groups (who is on the trip or not), you may still be at high-risk.

¹¹Particularly from international companies, or companies engaged in energy, defense/security, government contracts, information technology, advanced technology of any kind (agricultural, biotech, computing, space, etc.), natural resources or mining, or research & development. This list isn't comprehensive, if you think someone might think your business is interesting, then they probably will.

¹² For example, if you are an ethnic Chinese American visiting China, or an ethnic Russian visiting Russia, etc.

GENERAL SECURITY BEST PRACTICES FOR HIGH-RISK TRAVEL

Here are some general security tips for any devices you bring:

Before You Leave:

- **Have a plan for your devices and their security when traveling to high-risk countries.**
- Backup any devices you plan on bringing before leaving.
- Encrypt devices with strong passwords. **Change device passwords for your trip** from what you normally use and change them again on return. If officials inspect your devices, and especially if they make you give your password, change your passwords immediately afterwards.
- Disable Smart Lock (Android).
- If you will need email or other accounts when traveling, set up a temporary account to use for the trip. Don't send any sensitive information by email.
- Disable all file sharing (including Air Drop on iOS).
- Tape over integrated laptop cameras.
- Leave all unneeded access devices at home (like smart cards, RSA tokens, or a hardware token).
- If you need to bring a thumb drive or similar, encrypt it. Avoid bringing one if you can.

On Arrival:

- **Before you get off the plane to go through customs, ensure all devices are in airplane mode with all antennas turned off (Bluetooth/Wi-Fi), and then turn your devices off completely.** Keep them off while transiting customs and ideally through the airport. If you must turn a device on in the airport, keep it in airplane mode.
- If customs officials make you unlock your device, change your password when you get to the hotel.
- If a device leaves your sight while in customs, assume they took your data and added malware to your device to watch and steal from your future activity.

While There:

- Be aware that adversaries can use cameras, even possible hidden cameras in your hotel room, to see you type in your passwords.
- Keep your devices turned off when unattended, and in full airplane mode (cellular/Wi-Fi/Bluetooth) when you don't need internet access. Turn on what you need when you need it and turn it off again when done.
- Treat any removable media (CDs, thumb drives) or links/files you receive while traveling as hostile – they are likely to infect your devices even if they appear to be from a legitimate source.
- Don't use USB charging stations without a data blocker. Don't leave your data blocker unattended. If you do, assume it is also hostile (adversaries can similarly swap out chargers for hostile versions while you are out of the room).
- Avoid making/receiving voice calls, checking voicemail, or sending/receiving SMS messages. Use Wi-Fi calling or a virtual phone number service when you need to call someone. Use encrypted apps like Signal to communicate if available (some countries block encrypted messengers).
- Know that some services you rely on may be illegal or banned/blocked (Google, VPNs, WhatsApp).

On Return:

- Change the passwords for any accounts you accessed while traveling.
- Reset devices to factory and restore them from the backups you made before you left.
- Change your device passwords.
- Don't connect any "burner"/travel-only devices to any device or network you care about keeping secure.

BEST SECURITY FOR HIGH-RISK TRAVEL: DON'T TAKE YOUR DEVICES OR USE "BURNER" DEVICES

As discussed above, you should travel to these countries under the assumption that adversaries will closely watch you and steal any data you take with you. **The best choice is to leave your devices at home.** If you think you can go without your devices altogether, then do it.

If you cannot go without some devices, then buy cheap, clean versions for use on your trip(s). For phones, you may be best off buying one at the airport when you arrive or buy a cheap phone with prepaid service for the trip. If you bring or buy different devices, here are some tips:

- 1) If you need a tablet or laptop for a presentation or business, **put the smallest amount of information on it that you need, encrypt it, and don't access data (e.g. your email or password database) that you don't want compromised.** You can encrypt office or Adobe documents by adding a password to them or encrypt any files by archiving them (e.g. .zip, .rar) with a password. You could also store them in a VeraCrypt volume.
- 2) Don't take any contact information you don't need, and don't store it in your contacts – keep contacts in an encrypted file (e.g. a Standard Notes note).
- 3) When you return from your trip, don't connect your travel devices to your normal devices or networks, and reset them to factory settings at once.

GOOD SECURITY FOR HIGH-RISK TRAVEL: CLEAN YOUR DEVICES

If for some reason you cannot get new devices for your trip, the next best choice is to clean any device you need to take with you and restore it when you return:

- 1) First, **before traveling, back up the device.**
- 2) Next, reset it to factory settings (don't worry, you can restore from your backup when you return).
- 3) Set up the device for your trip by creating a new user account with a new password.
- 4) Add the minimal amount of data/information you need for the trip and encrypt it as described in #1 for best security, above.
- 5) When you get home, reset the device to factory settings again and restore it from your backup with your normal account.

MINIMAL SECURITY FOR HIGH-RISK TRAVEL: ENCRYPT AND TRAVEL SMARTLY

If you feel you absolutely must bring your normal devices, complete with all of your data on them, or don't think the threat is significant (in some cases you might be right – if you are a nurse traveling to Cancun for vacation, you are probably fine), then minimally practice the security practices for [routine travel](#) and [general security best practices](#) for high-risk travel. Make a backup and then remove any data you don't need.

You should still make a backup before you leave, change your passwords, then reset your device to factory settings on return, and finally restore from your backup at home. If any malicious software made its way onto your devices, this would get rid of it in most cases.

A travel Wi-Fi router is a particularly crucial tool in this scenario because it is the first and primary line of defense for your devices, combined with encryption and strong new passwords.

CONFIGURE BRAVE TO REDUCE TRACKING

Download and start using Brave to protect your online privacy.

GET BRAVE

Firefox is the Checkup's recommended browser for all operating systems. It offers exceptional levels of configuration to prevent tracking. For users uncomfortable with leaving the feel of Google Chrome, Brave is a good alternative because it is based on Google Chrome's source code. As a browser marketed to the privacy community, it also requires less configuration than Firefox to get to it to significantly reduce tracking. It's available on iOS and Android, as well.

It's also useful if you frequent websites that don't work well with Firefox.

Whatever you do, don't enable Brave Rewards. It's essentially an advertising experiment. We're trying to avoid things that can track us, and while it's fairly private, it's something to avoid.

For desktops/laptops, get Brave here: <https://www.brave.com>. Mobile devices can download it from the App Store or Google Play Store, respectively.

DESKTOP CONFIGURATION

Initial Setup:

- When you first launch Brave, it will guide you through a "Welcome Tour." Use the white Next button to navigate.
 - o On the second screen, you can optionally import bookmarks from your old browser by selecting it and importing. When you're done, move on.
 - o The third screen explains Brave's analytics. We're going to disable these later. Hit next.
 - o **Select your default search engine – choose DuckDuckGo or StartPage.**
 - o **Hit the Done button** (without enabling Brave Rewards).

Next, click "customize" at the bottom of the screen. **Toggle off sliders for: show sponsored images, Brave Rewards, and Binance.** You can also remove anything else you don't want.

Next, click the setting "gear" icon next to customize at the bottom of the screen.

From the **Settings Menu**:

- You can make Brave your default browser by clicking the white "make default" button.
- Under "On Startup," recommend you select "Open a new Tab Page." Opening old browser sessions can cause unwanted leaks. Or, set a home page to DuckDuckGo or StartPage if you want.
- Under the Appearance header, **toggle on "hide Brave Rewards button."** You probably also want to toggle on "show bookmarks" for the bookmarks toolbar.
- Under the Shields header, **select the radio button for "Advanced View."**
- * Just above Look & Feel, use the dropdown set Fingerprinting to "Block all fingerprinting."
- **Under the Social Media Blocking header, toggle all off.** If you haven't yet gotten rid of some Google or Facebook single sign-ons, then keep those turned on until you have done that.
- Under the Extensions header, **toggle off Hangouts Component.** Also **recommend toggling off "Private Window with Tor"** if you aren't very familiar with how Tor works.

Brave Configuration Guide (front)

The Complete Digital Privacy Checkup – May 2020

- Tap **"additional settings"** at the bottom of the page.
- Under the Privacy and Security header:
 - o Ensure **"autocomplete searches and URLs"** is toggled off.
 - o Set **"WebRTC IP Handling Policy"** to **"disable non-proxied UDP"**
 - o * **Toggle off "automatically send completely private product analytics to Brave"**
 - o Ensure **"help improve Brave's features and performance"** is toggled off.
 - o * **Toggle off "allow sites to check if you have payment methods saved."**
- Under the Autofill header, if you use a password manager, **select each of the three** (passwords, payment methods, addresses and more) and **toggle off all sliders**.
- Under the System header, **toggle off "continue running background apps when Brave is closed."**
- **Finally, in the address bar, type in:** `brave://flags/#dns-over-https` and hit enter. **Set the top setting, Secure DNS Lookups, to enabled.**

EXTENSIONS (DESKTOP AND ANDROID)

Next, click the hamburger menu icon in the top right of the screen (the three horizontal parallel lines). **Then select Extensions.**

If there are any extensions already listed here (and that are not listed below), recommend you remove them. Extensions can be powerful, but should be used sparingly to prevent fingerprinting, and bad extensions can track you or worse.

Next, click the link in the middle of the page for "Web Store." It will take you to:

<https://chrome.google.com/webstore/category/extensions>

Search for extensions in the top left search bar on the page. When you find them. Add them to Brave by click the large blue **"Add to Brave"** button, and then clicking the **"Add Extension"** button in the popup window. **You want to add the following extensions:**

- **Privacy Badger** offered by eff.org.
- **uBlock Origin** offered by Raymond Hill.
- **Your password manager's extension** (e.g. Dashlane, LastPass, BitWarden).

HTTPS Everywhere is not necessary in Brave because Brave does this on its own.

BRAVE FOR IOS/IPADOS (...and Android)

Download Brave from the app store and launch it. It will walk you through set up:

- * Tap either **DuckDuckGo** or **StartPage** and hit the save button.
- Tap continue.
- * **For Brave Rewards, tap "skip."**

Now, **enter settings by tapping the three horizontal dots in the bottom right corner, and select settings:**

- Toggle off **"Save Logins."**
- Tap **Brave Rewards, and then toggle on "Hide Brave Rewards Icon."**
- * **Toggle on "Fingerprinting Protection."**

Android settings should be essentially the same.

CONFIGURE FIREFOX TO REDUCE TRACKING

Download and start using Firefox to protect your online privacy.

GET FIREFOX

Firefox is the Checkup's recommended browser for all operating systems. iOS/iPad OS users will not have as many configuration options (iOS does not allow about:config tweaks or browser extensions), but will still gain a considerable reduction in tracking by switching from Safari while balancing usability. For a more private, but less user-friendly, browsing experience, iOS/iPadOS users can try DuckDuckGo browser or Firefox Focus.

For desktops/laptops, get Firefox here: <https://www.mozilla.org/en-US/firefox/new/>

Mobile devices can download it from the App Store or Google Play Store, respectively.

Jump to: [Basic Configuration](#), [Extensions](#), [Android](#), [iOS/iPadOS](#), [Advanced Configuration](#) (Desktop/Android)

Firefox Sync/Account: Firefox users can optionally sync their bookmarks, extensions, history, open tabs, and logins (you shouldn't need this because you should be using a dedicated password manager) using a Mozilla/Firefox account. If you created a Firefox Monitor account, you already have one. **This sync function is private – it is end-to-end encrypted so that Mozilla has no access to this information.** You can also enable 2FA for added protection.

BASIC CONFIGURATION (DESKTOP)

Once you've downloaded and installed Firefox, open it. When prompted, set it as your default browser. **To go to settings, click the three-parallel horizontal line "hamburger" icon in the top right of the screen, and then select "options."**

GENERAL SETTINGS

- Uncheck "restore previous session" under "startup" and ensure "always check if Firefox is your default browser" is checked.
- Scroll down, and under the "Digital Rights Management" header, **uncheck play DRM-controlled content.** You will probably not encounter any issues with this setting, but if you have trouble playing music or videos at sites you visit frequently, go back and check this box. This function can be used for tracking.
- Under "Firefox Updates" header, **ensure "automatically install updates" is selected and "use background service to install updates" is checked.**

- At the bottom, under the "Network Settings" header, **click the gray "Settings..." box.**

- o * At the bottom of this pop-up window, **check the "Enable DNS over HTTPS" box.** In the dropdown below this, you can optionally select another provider than Cloudflare, which is default. Both provided options are good (Cloudflare and NextDNS). Advanced users can set up another provider if they wish. **Click the gray OK box.**

Next, click **Home** on the left menu.

HOME SETTINGS

On the **Home** settings menu:

- Set your preferences for "Homepage and New Windows" and "New tabs." **Recommend: blank page for both.** Otherwise, set your homepage to either <https://duckduckgo.com> or <https://startpage.com>. Using the default Firefox Home is not recommended.
- **Under Firefox Home Content, uncheck all boxes.**

Next, click **Search** on the left menu.

SEARCH SETTINGS

- Under Default Search Engine header, **use the dropdown to select either DuckDuckGo or StartPage HTTPS.**
- **Under Search Suggestions header, uncheck all boxes.**
- Under one click search engines, select your preferences.

Next, click **Privacy & Security** on the left menu.

PRIVACY & SECURITY SETTINGS

On the **Privacy & Security** settings menu:

- ** Under the "Enhanced Tracking Protection" header, **select the Custom radio button.**
 - Check every box (Cookies, Tracking Content, Cryptominers, and Fingerprinters)
 - Next to Cookies, in the drop down, select "All third-party cookies (may cause websites to break)." If you have major problems with websites you frequent, you can step this down to "cross-site and social media trackers," but the all third party cookies setting provide significantly better tracking protection.
 - Next to Tracking Content, in the drop down, select "in all Windows." Then click the blue "reload all tabs" button.
- Below the custom box, select "only when Firefox is set to block known trackers" for "Send websites a 'do not track' signal." This is a bit counterintuitive, but more trackers ignore "do not track" signals and can use them to track you.
- * Under the "Cookies and Site Data" header, **check "delete cookies and site data when Firefox is closed."**
- Under the "Logins and Passwords" header, **uncheck all boxes** except "show alerts about passwords from breached sites."
- Under "Forms and Autofill" header, **uncheck autofill addresses.**
- Under "History" header, **use the drop down to select "use custom settings for history"**
 - Uncheck "remember search and form history"
 - Check "clear history when Firefox closes"
 - You can optionally select the "always use Private Browsing mode" box. This will keep Firefox from storing cookies and history all of the time. Contrary to what some people might think, that's all private browsing does – it doesn't prevent tracking or provide anonymity.
- Under the "Address Bar" heading, **uncheck all boxes** (Browsing History, Bookmarks, Open Tabs).
- ** Under the "Permissions" heading:
 - Ensure "Block pop-up windows" and "warn you when websites try to install add-ons" are both checked
 - For each permissions item (Location, Camera, Microphone, Notifications, Autoplay, and Virtual Reality), click the gray "Settings..." box, and then **check the box at the bottom of each of the popup windows to "Block new requests..."** also review

any of the listed sites in the box and remove them.

Then click the "save changes" box.

- **For Camera and Microphone:** most people don't need camera and microphone access in their browser and can safely block this. If you use your web browser for online video or audio calls, you need to leave this unblocked.
- **For Autoplay:** the Autoplay menu is slightly different from the others. At the top, **change default for all websites to "block audio and video"** and then save changes. You can set different settings for different sites you use by adding them to the list.

- ** Under the "Firefox Data Collection and Use" header, **uncheck all boxes.**

You can optionally set up/manage Firefox sync by click the Sync link on the left menu. If you use Sync, recommend you change the settings to only sync bookmarks, options, and add-ons. If you use these sync settings, you should only need to set up Firefox on one device (except for about:config settings, below), but check them to make sure.

When you're ready, click the **Extensions and Themes** box at the bottom of the left menu.

EXTENSIONS (DESKTOP/ANDROID)

First, you want to review any installed extensions and probably disable/delete them (unless they're in the below list). As discussed in the Checkup, extensions are powerful tools, but bad ones can be used to track you, and if you have too many, you make your browser easier to fingerprint.

To add extensions: Find extensions by searching for them in the search box at the top of the extensions page that says "search addons.mozilla.org." When you find it, click the extension, and then click the large blue "+ Add to Firefox" button. When asked for permission, click the blue "Add" box, and then for all of these extensions except your password manager, **check the "allow this extension to run in private windows" box** in the top right that pops up.

Extensions to add:

- Privacy Badger by EFF Technologists.
- HTTPS Everywhere by EFF Technologists.
- uBlock Origin by Raymond Hill.
- Your password manager's extension (e.g. Dashlane*, LastPass, 1Password*, BitWarden)
 - * Dashlane and 1Password extensions are installed from the desktop app and are not in the Firefox add-on store.

FIREFOX FOR ANDROID

Firefox for Android settings (all above about:config settings can be used if available). To go to settings, **tap the Menu hamburger button** (either below the screen or in top right), **then settings** (you may need to tap more first),

- **Privacy settings:** Tap Privacy.
 - o **Set Tracking Protection.** Tap Tracking Protection. **Ensure enhanced tracking protection is enabled:** turns on Tracking Protection for all tabs. If available, **set to strict.**
 - o **Disable Telemetry.** Tap Data Choices. **Uncheck all three** (Telemetry, Crash Reporter, and Mozilla Location Service).
- **Search settings:** Tap customize. Tap Search. **Set default search engine to DuckDuckGo or StartPage.**
 - o Ensure "show search suggestions" is unchecked.

Set about:config settings (below).

FIREFOX FOR iOS/iPadOS

Go to the settings menu by selecting the "hamburger" menu button in the bottom right hand corner, then tap **settings.**

- **Set Search Settings.** Tap Search.
 - o **Set default search engine to DuckDuckGo.** For StartPage, you can add a search engine at the bottom of the menu.
 - o **Ensure "Show search suggestions" is toggled off.**
- From the main settings menu, under the Privacy header:
 - o Tap Logins & Passwords and **toggle both off** (save logins and show in application menu).
 - o **Ensure "close private tabs" is toggled on.**
 - o * Tap Tracking Protection. **Ensure Enhanced Tracking Protection is toggled on. Set protection level to Strict.**
- * Under Support header, toggle off "send usage data"

ADVANCED CONFIGURATION (DESKTOP/ANDROID)

Completing the above processes will significantly improve your privacy on the internet, but you can get much more private by using **about:config** settings. These may look intimidating to a novice, but they're very simple to do.

First, in the Firefox address bar type: **about:config**

Second, click the blue "Accept the risk and continue" box. Don't worry, we're not going to change anything crazy here; all of the settings we'll be changing are well-tested and likely to be included in default installs of Firefox in the near future. You may find many are already set to the correct setting if you're using a later version of Firefox.

To check/change a setting: To change each setting, search for it (e.g. type: **privacy.firstparty.isolate**) in the search bar at the top of the browser window where it says "search preference name." To change it, click the toggle button to the far right of it (two half arrows pointing in opposite directions).

The settings:

media.peerconnection.enabled (WebRTC) = false
Disables WebRTC, which can be used to provide your true IP address. If you use browser-based video or audio calling, you need to keep this set to true.

privacy.firstparty.isolate = true

privacy.resistFingerprinting = true

privacy.trackingprotection.fingerprinting.enabled = true

These three settings block attempts at browser fingerprinting.

geo.enabled = false

Disables all attempts at geolocation tracking.

media.navigator.enabled = false

Prevents sites from getting microphone/camera status information. Keep set true if you use browser-based audio/video calls.

network.cookie.cookieBehavior = (recommend: 4)

Sets Firefox's cookie policy. 4 is the "new cookie jar" policy, which significantly reduces tracking. If you have major problems with sites you visit regularly, try changing to 1 (block third party cookies).

network.cookie.lifetimePolicy = 2

Cookies will be deleted after each session.

dom.event.clipboardevents.enabled = false

Sites won't get notifications if you copy/paste/cut from a page.

browser.send_pings = false

The attribute would be useful for letting websites track visitors' clicks.

network.http.referer.XOriginPolicy = 1

network.http.referer.XOriginTrimmingPolicy = 2

These reduce header information that is forwarded to sites when you click links.

beacon.enabled = false

Disables sending additional analytics to web servers.

network.IDN_show_punycode = true

Helps prevent hard-to-notice phishing attacks.

webgl.disabled = true

WebGL is a potential security risk.

browser.urlbar.speculativeConnect.enabled = false

Disable preloading of autocomplete URLs. Firefox preloads URLs that autocomplete when a user types into the address bar, which is a concern if URLs are suggested that the user does not want to connect to.

Disable Firefox prefetching pages it thinks you will visit next:

network.dns.disablePrefetch = true

network.dns.disablePrefetchFromHTTPS = true

network.predictor.enabled = false

network.predictor.enable-prefetch = false

network.prefetch-next = false

Prefetching causes cookies from the prefetched site to be loaded and other potentially unwanted behavior.

SYNC ADVANCED SETTINGS ACROSS DEVICES

Went through all the trouble to set all of these and don't want to do it again on multiple computers? If you have [Firefox Sync set up](#) to sync options, it won't sync these settings by default, but you can force it to with another **about:config** setting:

services.sync.prefs.dangerously_allow_arbitrary = true

As the name implies, this is dangerous to leave set to true because it can break different versions of Firefox as they update at different times.

To avoid that, change this setting to true, let your devices sync, and when they're all synced, change it back to false. In testing, not all settings synced. So double check to be sure.

CONFIGURE AND USE SIGNAL MESSENGER

For messaging, voice, and video calls

CONFIGURING SIGNAL

Note: Menus/Settings may change/vary based on operating system and version. Settings based on iOS version.

- When creating account:
 - o **It is okay to grant permission to sync contacts with Signal.** Contacts are encrypted and the Signal service will not have access to them (it's complex how this is done, but it's basically cryptographic magic.)
 - o On Android, you can optionally choose to make Signal your default SMS application. Just be aware that SMS messages sent with Signal are not secure (just like all SMS messages).
 - o **It is okay to sync/backup Signal to the cloud.** This is done securely and the cloud provider cannot read these messages (unlike many other message apps when they get backed up to the cloud, including iMessage).
- On opening the app, click the top left icon
- Click "Privacy"
 - o **Recommend: Disable "read receipts" and "typing indicators"**
 - o * **Enable "screen lock"**
 - o **Enable "screen security"**
 - o **Disable "always relay calls"**
 - o **Disable "show calls in recents"** This keeps call records out of your less-secure phone's call log.
 - o **Disable "send link previews"**
 - o * **Enable "Registration Lock"** – this prevents someone else from registering an account with your phone number without this PIN. Set a six-digit pin. (It will also ask you to enter this every few days at first, and then every couple of weeks)
- From main settings menu, click "Notifications"
 - o Under "Notification Content," recommend change Show to **"Name only"**

USING SIGNAL

To start a message: From main menu, tap top right pencil icon. If you synced your contacts, anyone on Signal under those numbers will be here. You can select them and get started.

- **You can start a group conversation by tapping the three people with the + sign icon in the top right.**
- You can also find a contact by their phone number by tapping "Find by Phone Number" at the top.
- **Invite any missing friends to Signal by tapping "Invite Friends to Signal."** This will send them a message inviting them to download Signal.

Video/Audio calls: from the message screen, you can initiate a call by **tapping the top right phone icon.**

- **Once a call is initiated, you can turn on video by tapping the video camera icon.**

From the message screen, you will get additional options by clicking your contact's name/number at the top of the screen.

- Here you can **set disappearing messages**, forcing messages to delete on both ends of the conversation. You can set a time from 5 seconds to 1 week.

SAFETY NUMBERS: AUTHENTICATE YOUR CONVERSATIONS

From the message screen, click the phone number of your contact at the top of the screen

- Tap **"View Safety Number,"** which is a good idea to **compare with your contact, in person or over video.** You are verifying two things: 1) that this is the person you want to communicate with (authentication), and 2) that they have the same safety number (your conversation is encrypted at both ends). **When verified, tap "Mark as Verified."**
 - o In a Signal video call, you can do this by hitting the "<" in the top left of the screen, tapping your contact's phone number at the top, and then tapping "View Safety Number"
- From time to time, you may get a message that says "Identity Key Changed. Tap to verify new key." This means one of two things, but either way you should re-confirm identity visually with your contact and re-verify safety numbers:
 - o 1) The recipient got a new device and set up/installed Signal (most likely).
 - o 2) An attacker is trying to gain access to your Signal conversations (the reason you should re-verify).

Database Removal Checklist

Start from a Clean Slate by Removing Your Data from Data Brokers

OVERVIEW

This checklist will help guide you through the process of erasing most of the data that is in the hands of major data providers and data brokers. It is entirely optional, but it is something to consider if you want to start with a “clean data slate” now that you have privatized your digital life. **You should not start this checklist without having first completing all the steps of the Checkup.**

Data brokers like Spokeo or Pipl scrape public records to build profiles on people. Over time, they can accumulate a lot of information. You can ask them to delete it, and they will, but if you have not stopped the data at its source by following the Checkup, and then contacting major data providers to stop the flow of information from them, then the brokers will just turn around and rebuild your profile in six months.

So, you must start with the major data providers:

MAJOR DATA PROVIDERS

Credit Bureaus (you could also hypothetically request deletion, but most people need their credit histories):

- ☐ **Credit Prescreening:** Opt out of credit prescreening at: <https://www.optoutprescreen.com/>
- ☐ **Experian:** (1) Credit freeze. (2) Opt out of data sharing: https://www.experian.com/privacy/ opting_out (3) Submit CCPA request to opt out of sale of data: <https://experian.com/ccpa> (warning: if anyone knows for sure who is a resident of California, it's the credit bureaus).
- ☐ **Equifax:** (1) Credit freeze. (2) Opt out of data sharing: call 1-866-807-7461. (3) Submit a CCPA request to opt out of sale of data: <https://myprivacy.equifax.com/personal-info>
- ☐ **Transunion:** (1) Credit freeze. Opt outs through optoutprescreen website above. (2) Submit a CCPA request to opt out of sale of data: <https://www.transunion.com/consumerprivacy>

Other Major Providers:

- ☐ **Axciom:** Opt out: <https://isapps.axciom.com/optout/optout.aspx>
- ☐ **Dun & Bradstreet:** If you have a business and your home address is listed as your business address on Dun & Bradstreet, you need to re-register your business with your state under a new address. **CCPA do-not-sell request here:** <https://support.dnb.com/?PROD=CCPARightToOptOut>
- ☐ **Epsilon Data Management:** Opt out: <https://us.epsilon.com/marketing-data-summary-request>
- ☐ **Intelius:** Opt Out: <https://www.intelius.com/optout> (Intelius may be the most important name on this list. It feeds many of the brokers listed on the next page and also owns over 10 other data broker sites of its own – your opt out will cover all of those)
- ☐ **LexisNexis:** Opt out: <https://optout.lexisnexis.com/>
- ☐ **Oracle Data Cloud (formerly Datalogix):** Opt out: <https://datacloudoptout.oracle.com/#optout>
- ☐ **Other providers.** These are the major providers. Visit this website for a more comprehensive list with links to each: <https://www.stopdatamining.me/opt-out-list/>

Database Removal Checklist (front) – Data Providers

The Complete Digital Privacy Checkup Checklist – May 2020

DATA BROKERS

Now, the data brokers. Work through this list of opt-out links. You can also submit separate CCPA do-not-sell requests for each site – this would go a long way to stopping these sites in their tracks because they are in the business of selling your information:

- ☐ **Allareacodes.com:** https://www.allareacodes.com/remove_name.htm
- ☐ **Ancestry.com:** Requires you to create an account to delete within account settings: <https://www.ancestry.com> – you could try contacting the privacy officer at dpo@ancestry.com
- ☐ **Beenverified.com:** <https://www.beenverified.com/lifestyle/opting-out-of-beenverified/>
- ☐ **Callersmart.com:** <https://www.callersmart.com/opt-out>
- ☐ **Check-caller.net:** Go to <https://check-caller.net> search your phone number and click remove.
- ☐ **Checkthem.com:** <https://www.checkthem.com/optout/>
- ☐ **Familytreenow.com:** <https://www.familytreenow.com/optout>
- ☐ **IDTrue.com:** <https://www.idtrue.com/optout/>
- ☐ **Instantcheckmate.com:** <https://www.instantcheckmate.com/opt-out/>
- ☐ **Nuwber.com:** <https://nuwber.com/removal/link>
- ☐ **Peekyou.com:** <https://www.peakyou.com/about/contact/optout/>
- ☐ **Peoplebyname.com:** <http://www.peoplebyname.com/remove.php>
- ☐ **PeopleFinder.com:** <https://www.peoplefinder.com/optout.php>
- ☐ **Peoplefinders.com:** <https://www.peoplefinders.com/opt-out>
- ☐ **Peoplesmart.com:** <https://www.beenverified.com/app/optout/search>
- ☐ **Pipl.com:** <https://pipl.com/personal-information-removal-request>
- ☐ **Privateeye.com:** <https://www.privateeye.com/static/view/optout/>
- ☐ **Publicrecords.directory:** <https://publicrecords.directory/contact.php>
- ☐ **Publicrecordsnow.com:** <https://www.publicrecordsnow.com/static/view/optout/>
- ☐ **Peoplewhiz.com:** <https://www.peoplewhiz.com/remove-my-info>
- ☐ **Radaris.com:** <https://radaris.com/page/how-to-remove>
- ☐ **Spokeo.com:** <https://www.spokeo.com/optout>
- ☐ **Telephonedirectories.us:** https://www.telephonedirectories.us/Edit_Records
- ☐ **Truepeoplesearch.com:** <https://www.truepeoplesearch.com/removal>
- ☐ **Truthfinder.com:** <https://www.truthfinder.com/opt-out/>
- ☐ **USA-people-search.com:** <https://www.usa-people-search.com/manage>
- ☐ **Voterrecords.com:** (CCPA do-not-sell only) <https://voterrecords.com/contact>
- ☐ **Whitepages.com:** <https://support.whitepages.com/hc/en-us/articles/115010106908-How-do-I-edit-or-remove-a-personal-listing->

Database Removal Checklist (back) – Data Brokers

The Complete Digital Privacy Checkup Checklist – May 2020