a

DIGITAL EXHAUST OPT OUT GUIDE

For Law Enforcement & Their Families

VERSION 3.0

1 TABLE OF CONTENTS

2 DISCLAIMER

2.1 NAVIGATION

It is recommended you follow the order of this Guide as presented. Doing so will aid you with the reduction of your Digital Exhaust, particularly in securing your Web Browser, which is a critical part of removing your Digital Exhaust.

- To navigate the guide, open it as a PDF document in Adobe® Acrobat® application.
- Select "View > Show/Hide > Navigation Panes > Bookmarks" from the Adobe® Acrobat® main menu.

The Bookmarks panel appears on the left side of the screen in the navigation pane. Press the "Bookmarks" icon in the navigation pane to open the Bookmarks panel. If Bookmarks panel is open, then clicking on the icon will close it.

2.2 PURPOSE

The Digital Exhaust Opt Out Guide 3.0 supersedes version 2.0 which was published in November 2021 and is being updated as of June 2022. This Guide was created to mitigate risk for Law Enforcement employees and their families as it pertains to protecting their personal information, which is vulnerable to exploitation. This risk includes potential for threat actors to find, target, and track anyone affiliated with the Law Enforcement via use of open source, Internet-based services offering searches of data aggregated about the American public. To mitigate this risk, this Guide was created as a first-of-its-kind aid for the Law Enforcement Community in highlighting and presenting recommendations to reduce these vulnerabilities. This document is for informational purposes only. Questions about this document can be directed to the email address listed below in Section 2.6.

2.3 LIMITING LIABILITY

This Digital Exhaust Opt Out Guide was prepared as a collection of best practices to aid Law Enforcement employees. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, or process shown. Reference here to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed here do not necessarily state or reflect those of the United States Government or any agency thereof.

2.4 LINKS

The appearances of hyperlinks, which are external to Law Enforcement databases, are provided as a convenience and for informational purposes only; they are not an endorsement by the Federal Bureau of Investigation. The Federal Bureau of Investigation bears no responsibility for the accuracy, legality, or content of the external site or for next links. Contact the external site for answers to questions about its content. The links provided within this Guide are current as of the publication in June 2022.

2.5 CONTENT

No policy, PG or IPG may contradict, alter, or otherwise change the standards of your Law Enforcement agency. Nothing in this Guide supersedes existing law and/or Department of Justice policy. Precautions must be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

2.6 AVAILABILITY

If you have questions, concerns, or comments about the Digital Exhaust Opt Out Guide, please direct any inquiries to the email address **kc_digitalexhaust@fbi.gov**.

3 Traffic Light Protocol (TLP) Instructions

The Traffic Light Protocol (TLP) was created to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience.[1] It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST Standards Definitions and Usage Guidance, Version 1.0.[2]

3.1 Traffic Light Protocol Definitions

Color	When should it be used?	How may it be shared?
TLP: RED  Not for disclosure, restricted to participants only.	Sources may use **TLP: RED** when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share **TLP: RED** information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, **TLP: RED** information is limited to those present at the meeting. In most circumstances, **TLP: RED** should be exchanged verbally or in person.
TLP: AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use **TLP: AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share **TLP: AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP: GREEN  Limited disclosure, restricted to the community.	Sources may use **TLP: GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.
TLP: WHITE  Disclosure is not limited.	Sources may use **TLP: WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

3.2 How To Use TLP In Email

TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color must be in capital letters: TLP: RED, TLP: AMBER, TLP: GREEN, or TLP: WHITE.[3]

3.3 How To Use TLP In Documents

TLP-designated documents should indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color should appear in capital letters and in 12-point type or greater.[4]

3.4 TLP Dissemination Guidance

If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.[5]

4 THE DIGITAL EXHAUST OPT OUT GUIDE

Presently, Law Enforcement actively investigates a broad range of threat actors, many of whom have resources and technical abilities that can be used to target Law Enforcement employees and their families.

These threat actors will continue to exploit the ever-increasing variety, volume, and speed of data sources to target Law Enforcment employees and their families, which requires the deployment of preventative measures.

Digital Exhaust will continue to challenge Law Enforcement and their partners ability to successfully work in an environment where network devices, expanded bandwidth, and reduced latency, will hyper-enable technical surveillance networks creating near real-time situational awareness for an adversary further challenging operational security, force protection, and reducing overall risk to the Law Enforcement mission.

Perform these opt out steps to control your digital exhaust. Progress through the Guide in the order presented for best results.

5 WHAT IS DIGITAL EXHAUST?

Digital Exhaust is data on the Internet about you.[6] [7] It is all the information or "consumer data" a person creates as they interact with web sites and services. You create some of it and others create some of it about you.[8, 9] These data points are exploitable to find, target, and track you.[10] Your Digital Exhaust holds extremely sensitive information that names you and reveals your private activities. Controlling Digital Exhaust is possible but complex.[11] This document serves to make it easy, or at least easier.

5.1 WHY SHOULD YOU CARE?

Because ***your*** privacy matters. Consider the vast amounts of personal information that different services hold about us and be mindful of what you give other organizations access to.[12] The privacy choices you make can have lasting impacts on you and your loved ones for better or worse.[13] This guide is laid out for you in a way that is the key difference in aiding Law Enforcement employees and their families in opting out of their data and taking positive steps towards keeping their Digital Exhaust from repopulating and out of the hands of a variety of threat actors.[14]

5.2 WHY DO I NEED A GUIDE?

Every interaction you have with the internet and technological tools leaves a trace, and these traces can be valuable.[15] Heading into this blindly will consume and waste a lot of your time.[16] Not anymore. These preventative measures are simple enough to employ and use safely in everyday life, both physically and online, while comprehensive enough to deny spectrum access to threat actors who could gain important operational advantages at the expense of you – a Law Enforcement employee – or your family.[17]

5.3 WHERE DO I FIT INTO DIGITAL EXHAUST?

Here. This is you.

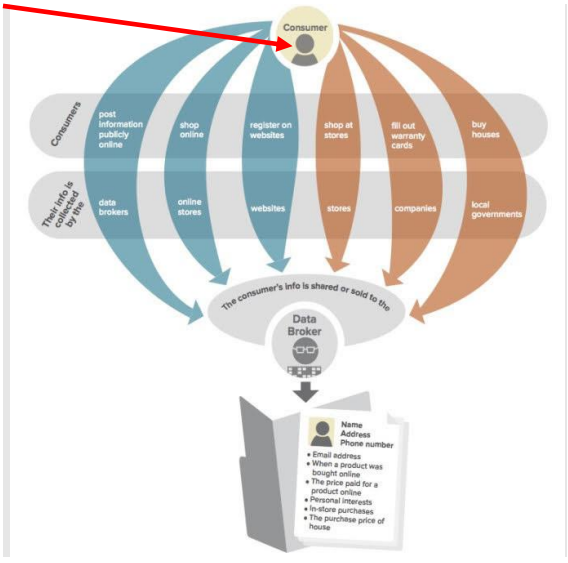


Figure 1. Digital Exhaust Ecosystem.

This is also you.

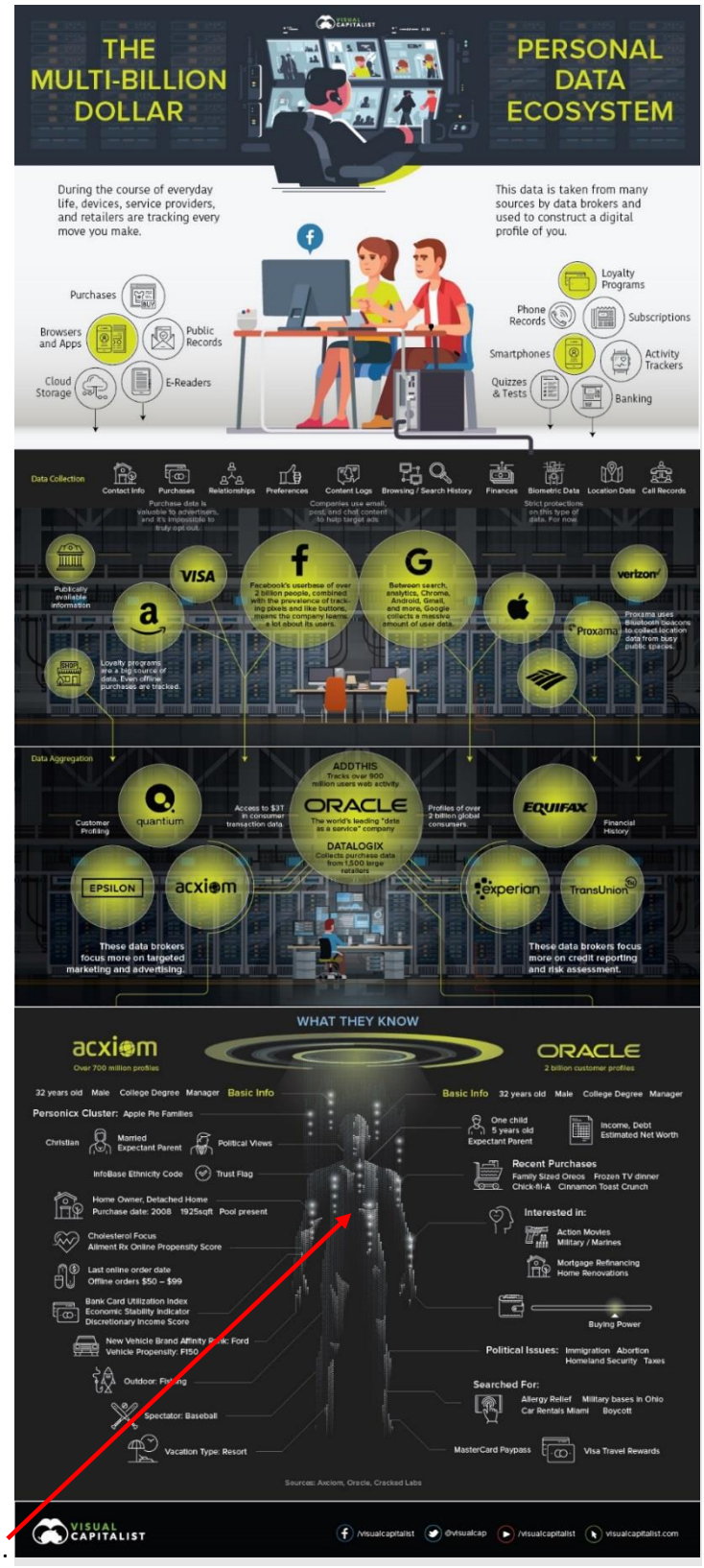
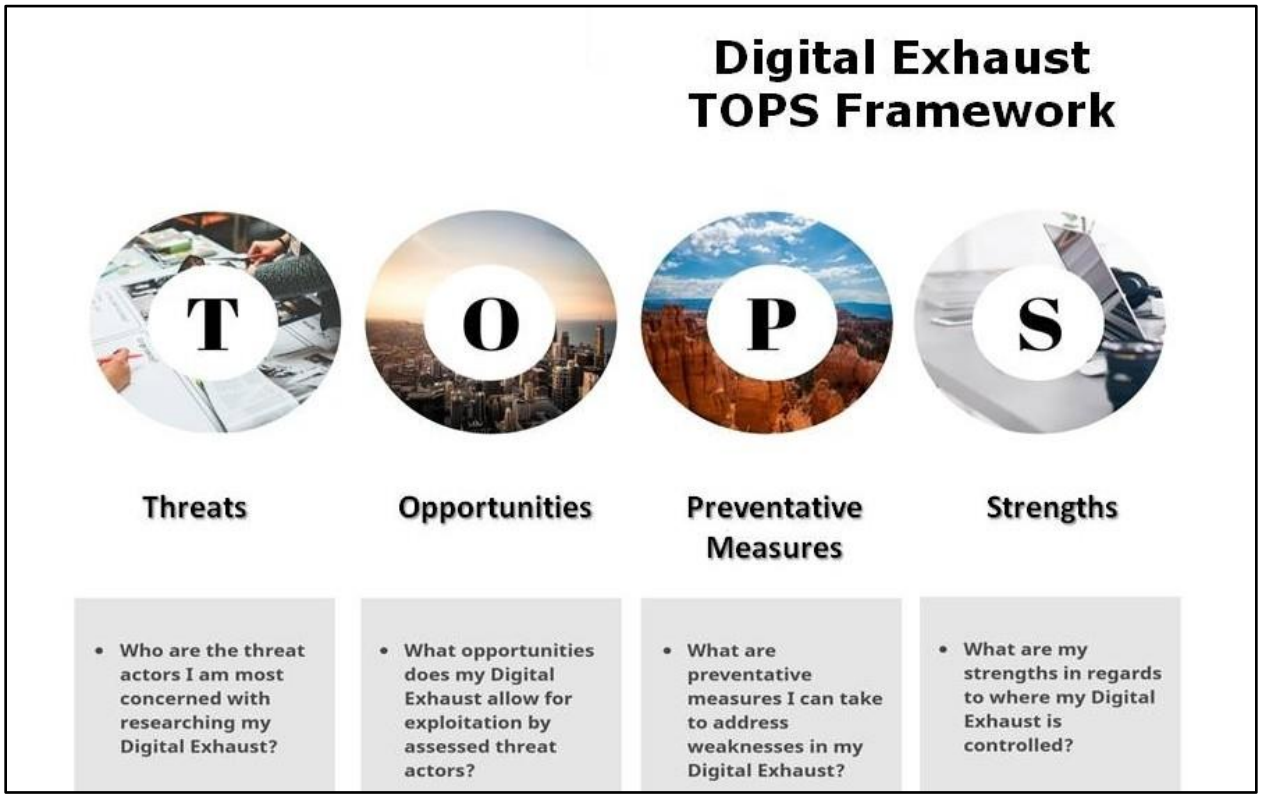


Figure 2. Digital Exhaust Ecosystem Players[18]

6 TOPS FRAMEWORK

To combat Digital Exhaust, it is recommended that users conduct a personal risk assessment of what they define as acceptable levels of risk for themselves and their family.

- This personal risk assessment often involves users assessing what pieces of their personal information form key assets, what they can remove online, what they cannot remove online, what they can obfuscate through deception and/or disinformation or simply allowing errors that may exist with Data Brokers and Data Aggregation websites to hold misinformation which also obfuscates an identity or exact personal information.
- Before a user can conduct a risk assessment, it is important they have the right mindset and then use a framework. One framework they can use is called **TOPS**.
- TOPS stands for **Threats, Opportunities, Preventative Measures** and **Strengths**. This framework is applied as follows:



6.1 THREATS

Using **TOPS** helps a user **SPOT** who they assess to be their biggest Threat Actors and prioritize where they invest their time to minimize the impact on their life.[19]

- ***"Who are the threat actors I am most concerned with researching my Digital Exhaust?"*** [20]

6.2 OPPORTUNITIES

Using **TOPS** always reminds a user of what they **POST** online.

- ***"What opportunities does my Digital Exhaust allow for exploitation by who I assess to be my Threat Actors?"*** [21]

6.3 Preventative Measures

Using **TOPS** helps a user **STOP** problems through mitigation.

- ***"What are preventative measures I can take to address my weaknesses in my Digital Exhaust?"*** [22]

6.4 Strengths

Using **TOPS** helps a user's decision making as it pertains to what **OPTS** I choose to execute.

- Do I opt out of data?[23]
- Do I opt into a service to help me control my personal information?[24]
- Do I opt to create disinformation which pollutes the data broker ecosystem?[25]
- Do I opt to do nothing and allow for misinformation to circulate to my advantage?[26]

It all factors into the question a user can ask through **TOPS**:

- ***"What are my strengths in regard to where my Digital Exhaust is controlled?"*** [27]

6.5 TOPS Output

As it pertains to user's Digital Exhaust, you can use this framework and choose what makes up your personal information's Key Assets.

- It is only then a user can begin assessing how their Digital Exhaust can be exploited and can begin building preventative or protective measures to mitigate their risk across a spectrum of tracking capabilities their family and they face personally.
- This framework can aid a user in understanding and shifting how they interact with their Web Browser, Mobile Phone and Mobile Apps, Social Media platforms and the totality of their privacy settings which can be used for their benefit. The primary issue for a user is and will always be the intent of who can exploit the totality of their Digital Exhaust and for what purpose.[28]

6.5.1 Personal Information: Key Assets

Personal Information key assets are critical pieces of a user's personal information that deserve special protection because of their destructive potential.[29]

- This Guide defines destructive potential as any key assets that if exposed publicly, could help targeting efforts by threat actors who could endanger a user's family or themself through intimidation or physical violence and/or damage my reputation or finances through identity theft or financial swindles.

6.5.2 Types Of Key Assets

How does a user show what key assets within their personal information require special protection?

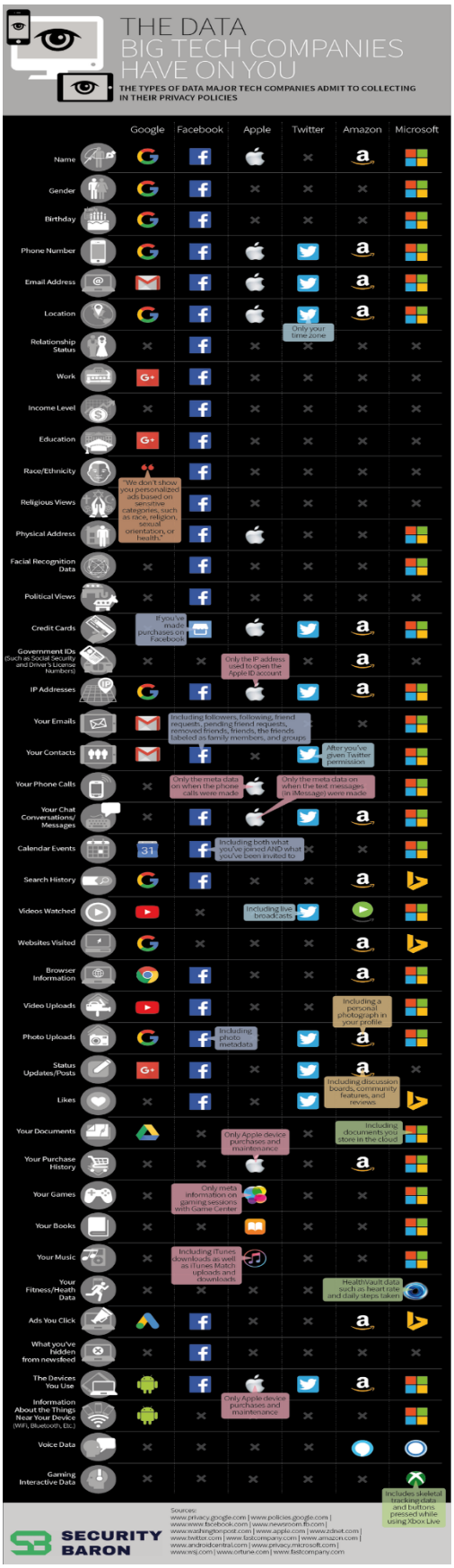
- For this Guide, the following key assets are the ones that users should apply preventative measures to include:
    - **First and Last Name**
    - **Date of Birth**
    - **Home Address**
    - **Social Security Number**
    - **Username(s)**
    - **E-Mail Address(es)**
    - **IP Address(es)**
    - **Telephone Number(s)**
    - **Credit Card Number(s)**

6.5.3 Preventative Measures: "Key Assets"

Once a user has named what threat actors they may meet, they can begin evaluating the totality of preventive measures and tailor them to be employed to thwart specific or all threat actors. These preventative measures may range from:

- Ensuring simple privacy settings are configured correctly.
- Mitigating physically consequential risks associated with their personal telephone number, home address and people search sites.
- Mitigating advanced threats such as ensuring a user has properly reduced any emissions of their Digital Exhaust on issues such as Online Behavioral Advertising which looks to use a user's Activity-Based Intelligence[30] to figure out their Patterns-of-Life[31], through Mobile Advertising[32], Behavioral Targeting[33], Categorical Targeting[34], Retargeting[35], Search Retargeting[36], Dynamic Ads[37].
- More subtle yet intrusive issues like ensuring a user has:
    - Mitigated Intelligent Tracking Prevention techniques[38],
    - Identified and disabled location tracking,
    - Disabled their photo's metadata,
    - Ensured they have deidentified their debit and credit card's ability to track their card transaction data[39],
    - And prevented their Web Browser from actively exploiting their Browser's unique fingerprint.

7 SECURING YOUR WEB BROWSER



7.1 HTTP VERSUS HTTPS

When you visit a website address, you will be met with either Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS). The latter choice uses a layer of encryption to enable secure communication between a browser and a server.[40]

The most important thing to remember is while HTTPS is best used by default in general browsing, when it comes to online purchases, it is crucial for protecting your payment details from eavesdropping and theft.[41]

To find out whether HTTPS is enabled, look in the address bar for "**https://**". Many browsers also show a closed padlock.[42]

7.2 TRACKING COOKIES

Tracking of browsing behavior is part of the daily routine of internet use.[43] Companies use it to adapt ads to the personal needs of potential clients or to measure their range.[44]

Cookies are a way to store user settings for websites locally in the browser.[45] For example, you might set your preferred time zone, which would result in a cookie being created in your browser with that setting.[46]

7.3 PREVENTING WEBSITES FROM STORING COOKIES

You can also set your preferences to prevent websites from storing cookies at all.[47] In order to do so, check out the following links which will provide you instruction on how to do so:

- **Firefox**
- **Chrome**
- **Opera**
- **Safari**
- **Edge**

7.4 CLEARING THE WEB BROWSER CACHE

Clearing out your cookie caches and browser histories can prevent ad networks from collecting too much information about you.[48] The easiest way to do so is to clear the cache and the following links will provide you instructions on how to do so:

- **Firefox**
- **Chrome**
- **Opera**
- **Safari**
- **Edge**

7.5 Browser Fingerprinting

Browser Fingerprinting, which is difficult to block, is based on the idea that every computer configuration is unique in some way.[49] Whenever you go online, your computer or device provides the sites you visit with highly specific information about your operating system, settings, and even hardware. The use of this information to identify and track you online is known as device or browser fingerprinting.[50]

A lot of that data is directly available to the sites you visit, usually for compatibility purposes. While cookie tracking works by placing a unique identifier on a person's web browser, fingerprinting takes place when a company creates a profile of your device's unique characteristics.[51]

All web browsers collect the following 10 types of data about you:

1. Your hardware and software.
2. Your connection information (to include your IP address and browser speed).
3. Your geolocation data.
4. Your browsing history.[52]
5. Your mouse or touch pad movements.
6. Your device's orientation (if using a Mobile browser).
7. Your information about which social networks you are logged into while browsing.[53]
8. Your installed fonts and which language you are using on your operating system.
9. Your image data.
10. Other technical data, including your screen size, touchscreen support, user agent, status of the Do Not Track (DNT) header, and more.

7.5.1 Browser Fingerprinting Test Websites

Much like a human fingerprint, browser fingerprints are a very specific identifier. If you are concerned about privacy, you need to be aware of how browser fingerprinting works, and what you can do to protect your data privacy.[54] The websites listed below are good resources to do so.

Service	Website
Electronic Frontier Foundation	https://coveryourtracks.eff.org/
Device Info	https://www.deviceinfo.me/
Browser Audit	https://browseraudit.com/
Browser Leaks	https://browserleaks.com/
IP Leak	https://ipleak.net/
Am I Unique	https://amiunique.org/

7.6 Web Browser Extensions and Add-Ons

Google Chrome and Mozilla Firefox supply straightforward ways to combat this including the use of add-on "extensions" which serve you by building layers of security into those browsers.

- Visit the articles at the URLs below for advice about these types of extensions then view the sample user extension setups for Chrome and Firefox to get a feel for how you can control collection on your 10 data types.

NOTE: The Guide suggests adding the extension found below as Protect My Choices **first** on all your browsers then adding Ghostery **second** followed by others.

- This order will first opt your browsers out of interest-based advertising (aka online behavioral advertising) then, second, protect them by blocking tracking ads altogether.

Be sure to test your browser after setup of add-on extensions to detect any continued unwanted collection or transmission of your data.

This can be done via open-source tools like Webkay (What Every Browser Knows About You) and Panopticlick; the URLs for these websites are available in Section 3.1.2.

7.7 Browser Extensions and Privacy

Some browser extensions track your private shopping behavior and collect data like order history and items saved in your Amazon cart.

- To protect your privacy and security, please refer to the links listed below and follow the instructions supported the specific browser of your choice to remove a harmful extension.[55]

- **Chrome** [56]
- **Firefox** [57]
- **Safari** [58]
- **Edge** [59]
- **Opera** [60]

8 Online Behavioral Advertising

Also called "Interest-based advertising", online behavioral advertising targets users with ads based on third-party predictions of their interests and preferences.[61] These predictions are based upon data collected from their devices' web viewing behavior over time and across non-affiliated websites.

- You can control some of this collection via your web browser's privacy controls, by choosing to Opt Out from the online behavioral advertising services run by the Network Advertising Initiative (NAI) and Digital Advertising Alliance (DAA), and by resetting your mobile advertising identifier.[62]
- Further information about online behavioral advertising is available at the Association of National Advertisers at **URL**.[63]
- You can also enable your browser to run a privacy tool like Ghostery, which blocks advertising attempts to gain access to your information. Ghostery can be read about at the **URL**.[64]

8.1 Browser Privacy Controls

Platform	Browser	Privacy Advice
Desktop	Chrome	http://support.google.com/chrome/bin/answer.py?hl=en&answer=95647
	Firefox	http://support.mozilla.org/en-US/kb/Enabling and disabling cookies#w_how-do-i-change-cookie-settings
	Internet Explorer	http://windows.microsoft.com/en-US/internet-explorer/delete-manage-cookies#ie=ie-11
	Safari	https://support.apple.com/guide/safari/manage-cookies-and-website-data-sfri11471/mac
	Opera	http://blogs.opera.com/news/2015/08/how-to-manage-cookies-in-opera/
Mobile	Chrome	https://support.google.com/chrome/answer/2392709?hl=en
	Firefox	https://support.mozilla.org/en-US/kb/clear-your-browsing-history-and-other-personal-dat
	Internet Explorer	http://www.windowsphone.com/en-us/how-to/wp7/web/changing-privacy-and-other-browser-settings
	Safari	https://support.apple.com/en-us/HT201265
	Opera	http://blogs.opera.com/news/2015/08/how-to-manage-cookies-in-opera/
	Silk	http://www.amazon.com/gp/help/customer/display.html?nodeId=201730580
	Android Browser	Click top right corner with three dots, Settings, Privacy

8.2 Online Behavioral Advertising Services

Service	Opt Out
Network Advertising Initiative (NAI)	http://optout.networkadvertising.org/?c=1
Digital Advertising Alliance (DAA) WebChoices Tool	http://www.aboutads.info/choices/
AppChoices (Mobile Apps)	http://www.aboutads.info/appchoices

9 MOBILE PHONES AND MOBILE BROWSING

For most of us, our mobile phone is the single most valuable tool we carry, but it can also be used against us by malicious actors.[65] It is important to know what your phone holds[66] and how it can also make you vulnerable to attacks.[67]

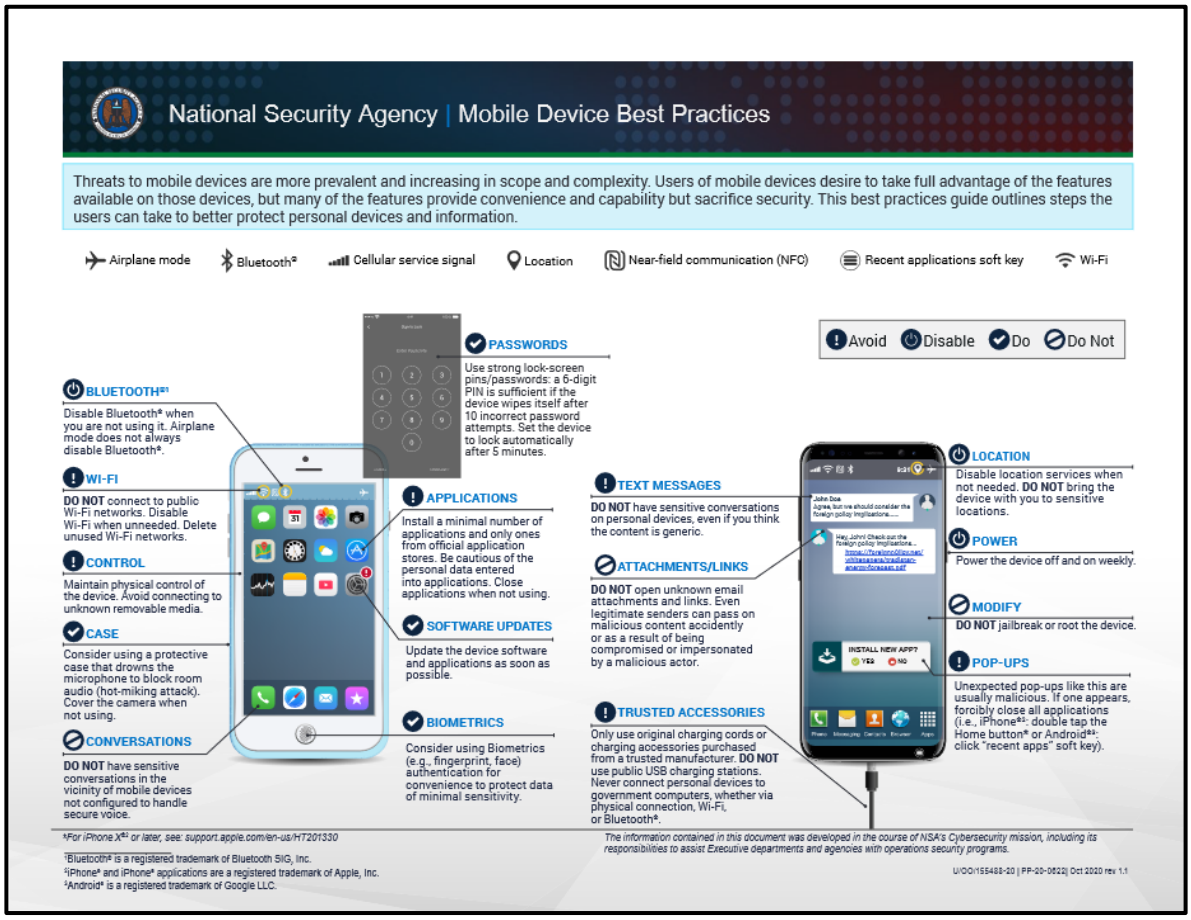


Figure 3. *National Security Agency | Mobile Device Best Practices*[68]

- Mobiles phones have a variety of sensors and software, which generate data useful for finding and tracking you.[69, 70, 71, 72, 73]
- Check your location settings and advertisement settings via advice below. Be aware smartphone apps could also leak your personal data to include your location.[74, 75, 76, 77, 78]
- Privacy advice for safely downloading smartphone apps can be read at the following **URL** and below for Apple and Android technology settings.[79]

9.1 Mobile Phones

Platform	Technology	Privacy Advice
Android	Location Settings	https://www.digitaltrends.com/mobile/android-privacy-guide/ *Pixel only:* https://android.gadgethacks.com/how-to/20-privacy-security-settings-you-need-check-your-google-pixel-0193251/
	Limit App Store Interest-based Ads	https://support.google.com/googleplay/android-developer/answer/6048248?hl=en#zippy=%2Chow-to-opt-out-of-personalized-ads
	Limit Ad Tracking	https://support.google.com/accounts/answer/2662856?co=GENIE.Platform%3DDesktop&oco=1#everywhere
Apple	Location Settings	https://support.apple.com/en-us/HT207092
	Limit Ad Tracking	https://support.apple.com/en-us/HT202074
	Limit App Store Interest-based Ads	https://support.apple.com/en-us/HT202074
Apple and Android	Reset Mobile Advertising Identifier	https://www.adcolony.com/privacy-policy/finding-advertising-id/

9.2 FCC Smartphone Security Checker

This tool was designed to help the many smartphone owners who are not protected against mobile security threats. To use this tool, choose your mobile operating system at the following **URL** and then follow the customized steps to secure your mobile device.[80]

9.3 Mobile Browsing

Online privacy is a major concern in the tech world, and by far some of the biggest privacy issues arise when you browse the internet, even if you use a mobile browser.[81] Having a solid understanding of these privacy settings is critical to reduce your Digital Exhaust as a user will be exposed to many techniques to track them around the web due to cookies, your IP address, and other device-specific identifiers.[82]

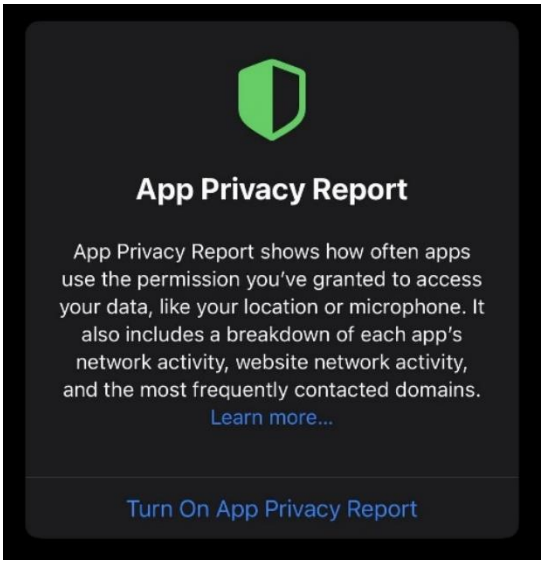
Platform	Technology	Privacy Advice
Browser	Chrome	https://defendingdigital.com/google-chrome-security-privacy-guide/
	Firefox	https://restoreprivacy.com/firefox-privacy/
	Safari	https://defendingdigital.com/apple-safari-security-privacy-guide/
	Brave	https://support.brave.com/hc/en-us/articles/360017989132-How-do-I-change-my-Privacy-Settings-
	Edge	https://privacyinternational.org/guide-step/4333/edge-adjusting-settings-enhance-your-online-privacy
	Opera	https://help.opera.com/en/latest/security-and-privacy/
Search Engine	Google	https://www.cnet.com/google-amp/news/do-you-care-about-online-privacy-then-change-these-browser-settings-immediately/
	DuckDuck Go	https://spreadprivacy.com/how-anonymous-is-duckduckgo/
	Google	https://www.pcworld.com/article/3299042/privacy/google-privacy-checkup-faq.html https://www.pcworld.com/article/3315701/mobile/how-to-delete-google-search-history.html

9.4 iPhone Privacy Settings

Apple in June 2021 introduced the latest version of its iOS operating system, iOS 15, which was released in September 2021. Apple's iOS 15 is the latest version of the mobile operating system and features several new privacy features that were not previously available with older operating systems. The newest privacy features are as follows:

9.4.1 App Privacy Report

With the rollout of iOS 15.2, Apple has enhanced the App Privacy Report feature which allows users to glance at the various information the installed apps accessed. The App Privacy Report holds a lot of data, some of which can be confusing, but one thing is clear: with a content blocker, you will be tracked much less by companies monetizing your activity to sell ads.



While Apple's Intelligent Tracking Prevention feature blocks some trackers, there are other ways to be tracked.[83] Using the App Privacy Report can help you find which websites or apps are tracking you the most and may lead you to change your behavior. Content and tracker blockers can help prevent companies from building profiles based on your activity and enhance your privacy.[84]

With the App Privacy Report feature in iOS 15.2 and iPadOS 15, you can quickly look at the various information accessed by these apps and revoke certain permissions for them if needed. It gives you the chance to see exactly what your apps are doing and decide if they are accessing information they should not.[85] The App Privacy Report feature displays app information for the last 7 days, divided into different sections to include Data and Sensor Access, App Network Activity, Website Network Activity and Most Contacted Domains.[86] [87]

9.4.1.1 Data and Sensor Access

Data and Sensor Access shows how many times and when an app accessed privacy-sensitive data or device sensors in the past 7 days. This may include details about an app's access to Location, Photos, Camera, Microphone, Contacts, and more. You can tap each app and data type to learn more.

Apple apps use Contacts data in several ways on your device to supply features to you. For example, Apple TV, Apple Music, Apple Podcasts, Fitness, and Apple Books use your Me card from Contacts to display your profile photo in those apps. Notes, Reminders, and Messages personalize your experience on each device with names from your Contacts. Camera and Photos use Contacts to show people in photos for albums, Memories, and other features that are personalized on your device. Fitness and Health use Contacts to enable sharing features. Calendar uses Contacts to display birthdays. In these cases, contact names and photos are kept on your device and are not sent to Apple.

9.4.1.2 Website Network Activity

This category displays all domains contacted by the websites you have recently visited using Apple's own Safari browser. It is not unusual for your device to connect to certain domains but now you can see if any unusual domains appear outside of your normal browsing patterns. Website Network Activity shows domains that have been contacted by websites you have visited within apps in the past 7 days.

9.4.1.3 App Network Activity

The app network activity is like the website network activity, but for apps. This activity helps you track all the domains your downloaded apps have used/contacted in the last 7 days. This report will allow you to see which websites you have visited with these apps or if these apps have collected tracking activity.

9.4.1.4 Most Contacted Domains

If you simply want to be informed about the most contacted domains of the apps you have installed on your iPhone with iOS 15, then the "Most Contacted Domains" feature is just what you need. As the name suggests, it is a common list of the most contacted domains. Usually, these domains are filled with various trackers and analytics domains.

9.4.1.5 How To Enable App Privacy Report

Settings > Privacy > **App Privacy Report** > then turn on **App Privacy Report**.

9.4.2 Hide Your IP Address From Trackers

Safari can now cloak your IP address from trackers on websites, making it impossible for your browsing to be logged.[88]

- Go to **Settings > Safari** and set **Hide IP Address** to **From Trackers**.

9.4.3 Apple's iCloud Private Relay

If you have an iCloud+ subscription, Apple has just given you a great reason to use the Safari browser -- iCloud Private Relay. This is like a VPN in that it sends your web traffic through other servers to keep your location secret.[89] Apple is introducing Private Relay technology as ISP anti-tracking solution. Altogether with the Application Transport Security requirement for all third-party apps, it supplies security and privacy cover for network communication on an extremely elevated level, resolving one of the main pains of VPN.[90] Despite the fact, that Private Relay technology does not allow to change browsing location, it resolves ISP anti-tracking issue well.[91]

9.4.3.1 Enable iCloud Private Relay In Settings

Apple's iCloud Private Relay is simple to use. iCloud+ subscribers can turn on the service from iCloud settings on any Apple device with iOS 15, iPadOS 15, or macOS Monterey or later.[92]

- On an iPhone, iPad, or iPod touch, go to **Settings > [your name] > iCloud >Private Relay**.
- On a Mac, go to **System Preferences** > **Apple ID** > **iCloud** > **Private Relay**.
- Once it is enabled, users can choose how they would like Private Relay to convey their location.
    - **"Maintain general location"** means that Private Relay will choose Relay IP addresses that map to a city-level area consistent with where the user is connecting from. This allows sites to use the Relay IP address to show correct localized content.
    - **"Use country and time zone"** means that Private Relay will choose Relay IP addresses across a broader, more regional area to give added privacy. All Relay IP addresses will still map to the user's original country and time zone.

9.4.3.2 iCloud Private Relay: Wi-Fi Network

1. Go to **Settings > Wi-Fi > Information**
2. Turn **iCloud Private Relay** on or off.

If you turn off **iCloud Private Relay** for a Wi-Fi network on your iPhone, **iCloud Private Relay** is turned off for this network across all your devices where you are signed in with the same Apple ID.[93]

9.4.3.3 iCloud Private Relay: Cellular network

1. Go to **Settings** > **Cellular**, then do one of the following:
    - *If your iPhone has a single line:* **Cellular Data Options**.
    - *If your iPhone has multiple lines:* **Select a line** (below Cellular Plans).
2. Turn **iCloud Private Relay** on or off.

9.4.4 Stopping Email Trackers

Protect Mail Activity is a feature built into the Mail app that prevents people from knowing if emails have been opened.[94]

- To enable this feature, go to **Settings > Mail > Privacy Protection** and enable **Protect Mail Activity**.

9.4.5 iPhone Communication Safety Settings

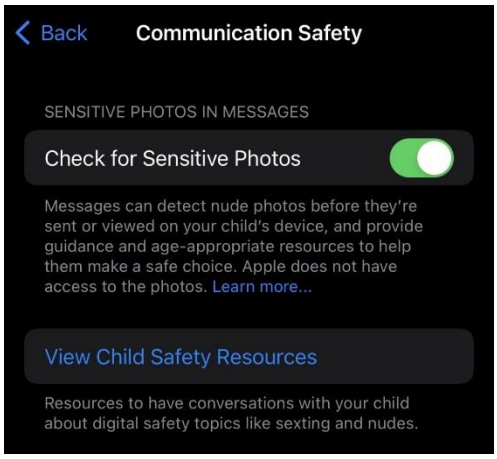
Apple is releasing a suite of features across its platforms aimed at protecting children online, including a system that can detect child abuse material in iCloud while preserving user privacy. Parents or loved ones can now turn on communication safety to help protect a child from viewing or sharing photos that have nudity in the Messages app. If Messages detects that a child receives or is trying to send this type of photo, Messages blurs the photo before it is viewed on your child's device and supplies guidance and age-appropriate resources to help them make a safe choice, including contacting someone they trust if they choose.[95]

Messages uses on-device machine learning to analyze image attachments and decide if a photo has nudity. The feature is designed so that Apple does not get access to the photos. The communication safety feature requires iOS 15.2 or later, iPadOS 15.2 or later, or macOS Monterey 12.1 or later, and is

available to child accounts signed in with their Apple ID and part of a Family Sharing group. This feature is off by default.[96]

9.4.5.1 How To Turn On Communication Safety in Screen Time

- On your iPhone, iPad, or iPod touch, go to **Settings** > **Screen Time**. On a Mac, choose **Apple menu > System Preferences**.
- Then click **Screen Time**. (If you have not already turned-on Screen Time, use parental controls to turn it on.)[97]
- Tap the name of the child in your family group.
- Then **Communication Safety > Continue**.
- Turn on **Check for Sensitive Photos**. You may need to enter the Screen Time passcode for the device.



9.4.6 Custom Alphanumeric Code

With the rollout of iOS 15, you can now generate a strong passcode using Custom Alphanumeric Code if you suspect someone knows your passcode.[98] To do so, complete the following steps:

- Go to **Settings > Face ID & Passcode** (or Touch ID & Passcode).
- Turn on **Face ID/Touch ID**.
- Turn on screen **Auto-Lock**.
  Go to **Settings > Display & Brightness > Auto-Lock** and set to 30 seconds or 1 minute.
- Make sure iOS is up to date.
  Go to **Settings > General > Software Update** and make sure **Automatic Update** is enabled.
- Keep all your apps updated.
  Go to **Settings > App Store** and make sure **App Updates** are enabled.

9.4.7 Built-In Authenticator

With the rollout of iOS 15, users have the option to use a built-in authenticator rather than choosing to use a third-party two-factor authenticator app.[99] If you choose to use this feature, simply follow the steps below:

- Got to **Settings > Passwords,** and then for each password entry, you can tap on it to get access to a choice called **Set Up Verification Codes…** which allows you to enter the information needed either using a setup key or QR code.
- Using a two-factor authenticator is far more secure than relying on SMS messages, so you should use this feature either using Apple's authenticator or another app to get the highest security.

9.4.8 Privacy-focused Apple Calendar Settings

While there is no known open-source reporting about Apple calendars being used by threat actors to target users through the creation of messages used in phishing schemes or social engineering attacks, the following URLs will help you ensure your Apple Calendars are configured properly.

Browser Privacy Control	URL
Apple Calendar (Share Calendars)	https://support.apple.com/kb/PH2690?locale=en_US
Apple Calendar (Stop Sharing Calendars)	https://support.apple.com/guide/icloud/stop-sharing-a-calendar-mm6b1a8f9f/icloud

9.4.9 App Store Personalized Recommendations

Click on the **Account Settings** button, which will prompt you for your passcode or a biometric identifier. Once in, look for the setting entitled **Personalized Recommendations**.

- If the switch is green, the settings is **enabled,** and your iPhone will send you Personalized Recommendations. Ensure the switch is not green to *disable* this feature.
- Apple describes Personalized Recommendations as "*when you download from a Store, or install an app on your Apple Watch, identifiers such as Apple logs your device's hardware ID and IP address along with your Apple ID. Apple further describes that they find ways use information about your browsing, purchases, searches, and downloads. These records are stored with IP address, a random unique identifier (where that arises), and Apple ID when you are signed into a Store"* at the following **URL**.[100]

9.4.10 Country/Region Settings

It is important to note that US users should ensure the Country/Region is set to the United States and not set to a different country.

- A misconfiguration of this setting risks having all your account's data transferred to another country beyond the protections afforded by the US Constitution AND may also directly expose it to threats from any government whose Intelligence or Law Enforcement services may or may not have means to decrypt what is stored in their country.
- Additional information on tips on how to ensure your safety when traveling to high-risk areas can be found at the following **URL**.[101]

9.4.11 Siri and Audio Data

In 2019, **Apple announced it would no longer listen to Siri recordings** without your permission. The company can only receive your audio data if you choose to opt in.

- If you opt in and later change your mind, go to your iPhone's **Settings > Privacy > Analytics and Improvements >** turn off **Improve Siri & Dictation**.
- You can also go to **Settings > Siri & Search**. Toggle off **Listen for "Hey Siri."**

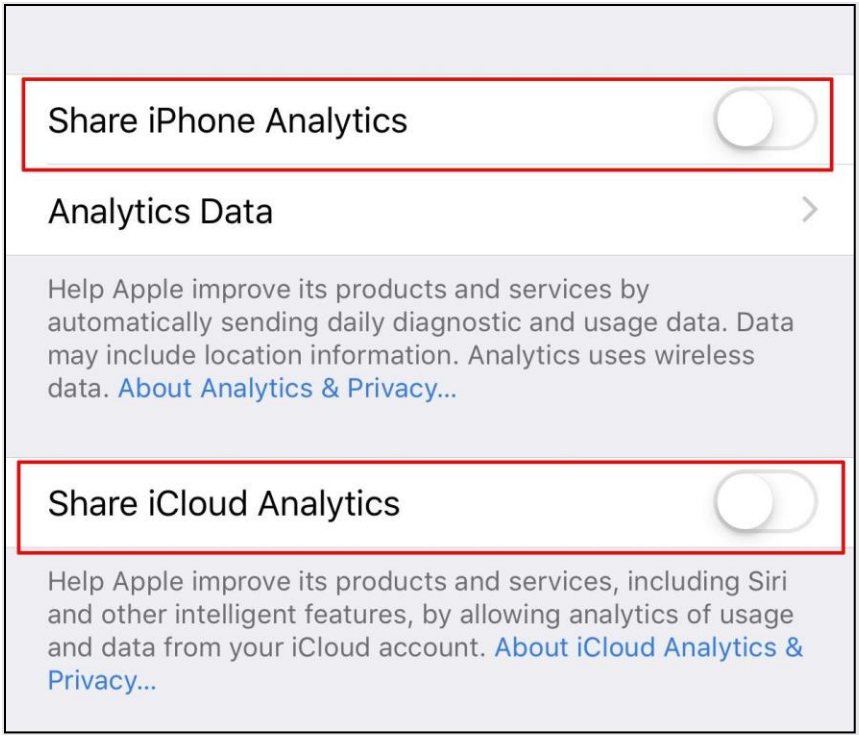
A feature that came with a previous iOS update lets you **delete all of your recordings**. In addition to this feature there are several other privacy options you can enable.

- On your iPhone, iPad, or iPod touch, open your **Settings > Siri & Search > Siri & Dictation History >** and select **Delete Siri & Dictation History**.
- On a HomePod, go to **HomePod Settings** in the Home app **> Siri History > Delete Siri History**.

9.5 iPhone Ads And Location Settings

This section guides you how to control your iPhone's **Analytics** and **Advertising**, **Location Services**, ability to deliver **Location-based Apple Ads**, track your **Significant Locations**, and ability to deliver **Personalized Recommendations** through your location. This **URL** will inform you how your iPhone shares analytics, diagnostics, and usage information with Apple.[102]

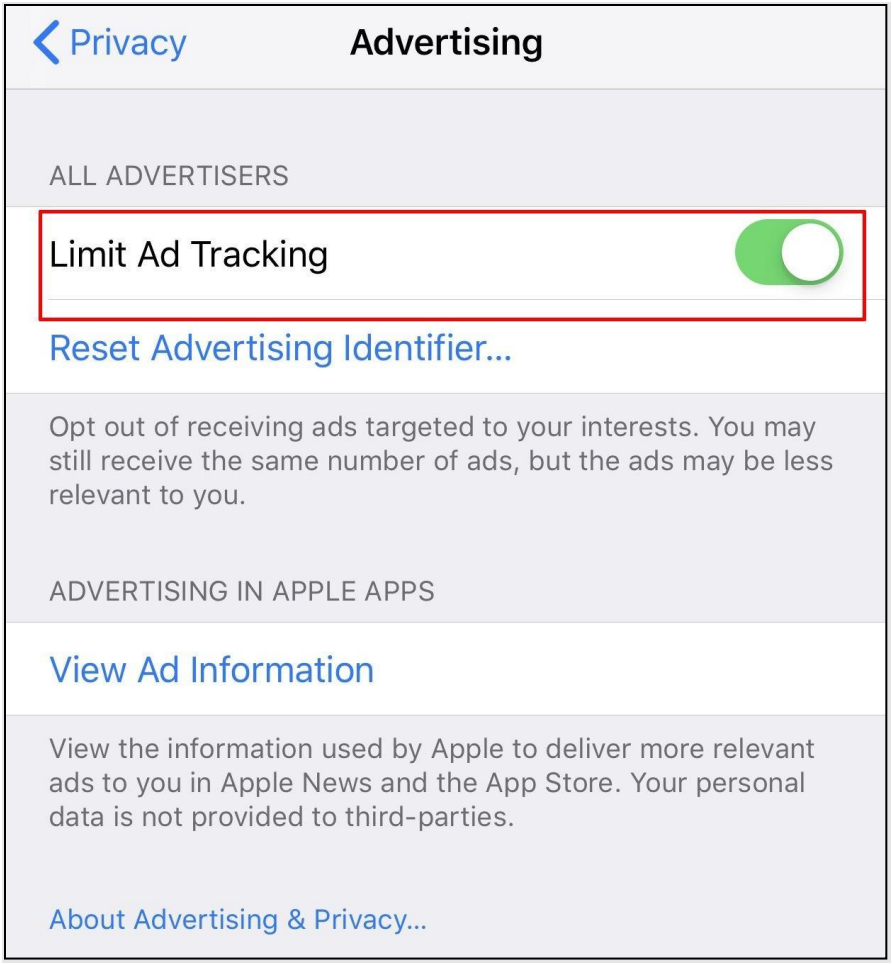
- With the rollout of Apple's new **iOS 15**, the following tips are still applicable though users have a greater ability to manipulate privacy settings within **iOS 15**.[103] This **URL** will inform you on some key features within **iOS 15** that will better enhance your iPhone Analytics.[104]



9.5.1 iPhone Advertising

Click on the **Reset Advertising Identifier** section periodically to ensure you are controlling what Apple describes as "Segments" of your personal information and data.[105] If you would like to know more about the information used by Apple to deliver relevant Apple ads to you in Apple News and the Apple App Store, click the **View Ad Information** section to view your personalized data.

- You can read more about “segments” at the following **URL**.[106]

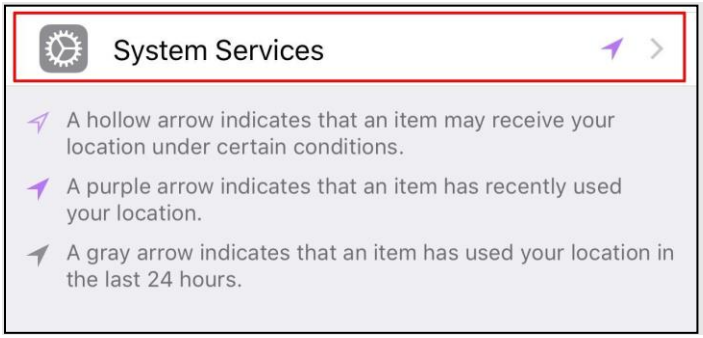


9.5.2 iPhone Location Services

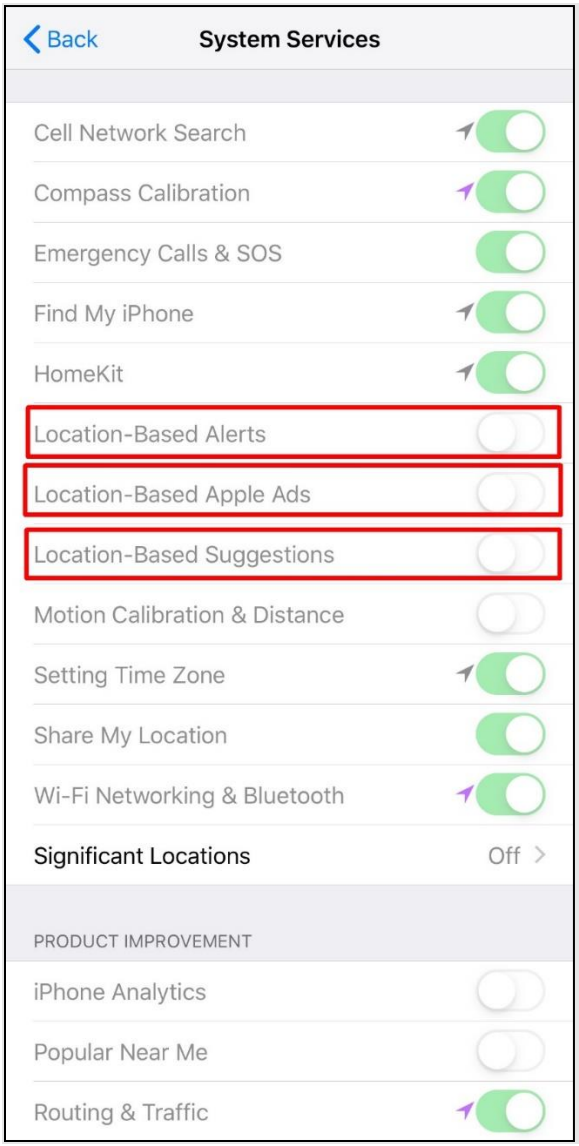
Open Settings and tap Privacy. You will now see the Location Services as shown in the graphic. According to Apple, Location Services uses GPS and Bluetooth (where available), along with crowd-sourced Wi-Fi hotspots and cellular towers to find the approximate location of your device.[107]

- The website also describes Apps won't use your location until they ask for your permission and you allow permission." Review this for yourself at the following **URL**.[108]
- Click on **Location Services** and you will see all the Apps your phone has installed and what type of access you have given each App about using your iPhone's location. You have three options available**: Always**, **While Using The App** and **Never**.
- What setting you use depends on your preferences so after you evaluate your App location settings, scroll to the bottom of the page, and look for System Services, as shown in the graphic.

9.5.3 iPhone Location-based Apple Ads



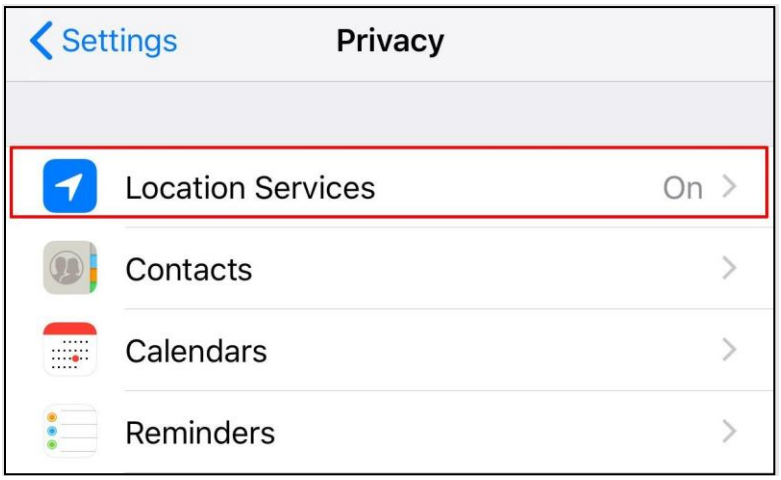
Then,



9.5.4 iPhone Significant Locations

The **Significant Locations** setting allows your iPhone to keep track of places you have recently been as well as how often and when you visited them.[109]

- Apple explains these data are "*encrypted and stored only on your device and will not be shared without your consent. It is used to provide you with personalized services, such as predictive traffic routing, and to build better Photos Memories*" at the following **URL**.[110]



9.5.5 Find My Network

Within iOS 15, the Find My app introduces new abilities to help locate a lost device that has been turned off or erased using the **Find My Network**.[111] Any trusted connections to a user can share their location with which will continuously live-stream their location to provide a sense of direction and speed.[112] There are also new Separation Alerts to notify a user if they leave an AirTag, Apple device, or Find My accessory network behind in an unfamiliar location.[113]

9.6 Android Privacy Settings

Your Android phone includes records of everywhere you go alongside most, if not all, of your digital communication and Internet search history.[114] The following section is designed to help users to understand and adjust privacy settings and reduce their Digital Exhaust.[115]

9.6.1 Android 12 Privacy Dashboard

Like most Android updates, Android 12 changes how some of the settings menus are categorized. Once you know your way around, though, you will be able to get to the Privacy Dashboard without any trouble at all.

App Drawer > Settings > Privacy > Privacy Dashboard

9.6.2 Connected devices

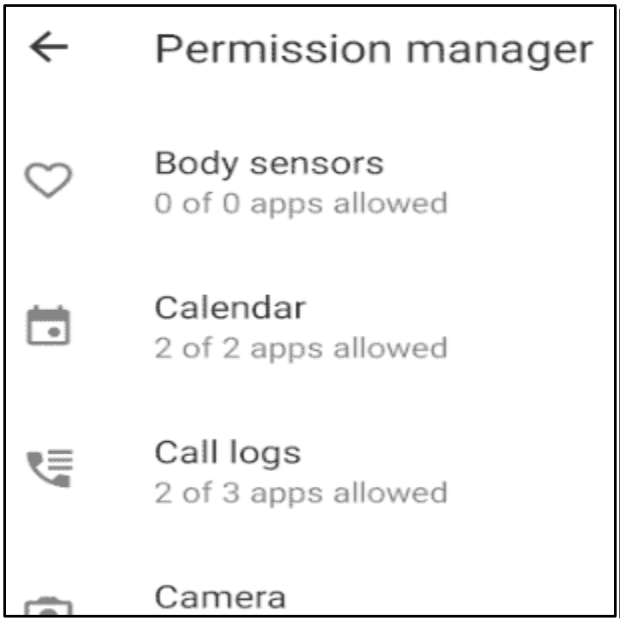
Settings > Connected Devices.

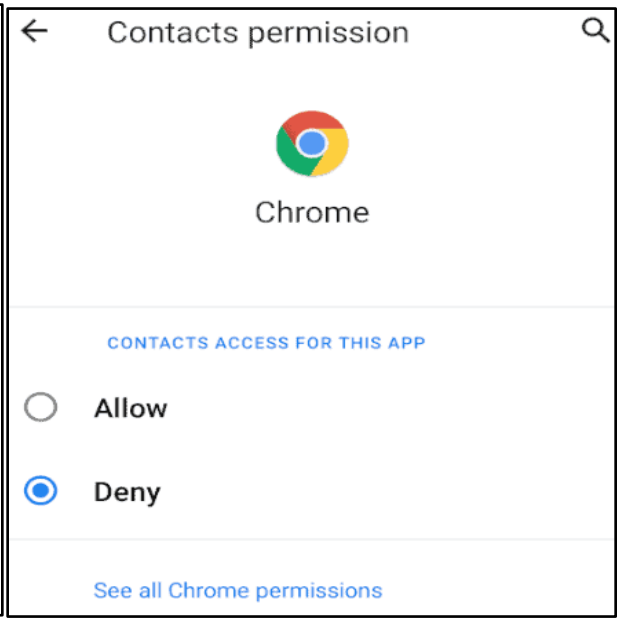
- If there are any connections you are not using right now, such as Bluetooth, tap them and toggle them **off**. Only enable connections when you truly need them. This limits the ways your device could be compromised and limits how your location can be tracked.[116]

9.6.3 Apps & Notifications

Settings > Apps & Notifications.

- **See All # Apps -** Go through the **App Info** list and for any that you do not truly need, select the app, then tap **Uninstall**. Many pre-installed apps cannot be uninstalled, so you will not see an **Uninstall** button. For those, you can tap **Disable** to turn the app off and hide it from your device.[117]
- **Permission manager** - Tap each permission (Body sensors, Calendar, etc.) to see the apps with that permission. If any app should not have the permission, select it, then hit **Deny**.
- **Advanced > Emergency alerts** - Toggle **on** any emergency alerts you want to receive.





9.6.4 Display

- In the top left, tap the **back arrow** until you are back to the *Settings* screen. Then, tap **Display**.
- Tap **Screen timeout**. Choose a brief time (it is recommended you choose ***1 minute*** or less). When you add a screen lock later, this will cause the screen to lock after a brief period of idle time, preventing others from using your device.
- Go back to the *Display* screen, then tap **Advanced**, then **Lock screen display**, then **Lock screen**. I recommend choosing **Don't show notifications at all**, because notifications can reveal sensitive data (messages, calendar reminders, etc.).
- Tap **Lock screen message**. Here you can set a message that shows on the lock screen. If a Good Samaritan finds your device, this will tell them how to contact you. However, do not give away

too much personal info, because a nefarious person could use it against you. Do not put your home address. I recommend putting a phone number and/or email address.

9.6.5 Privacy

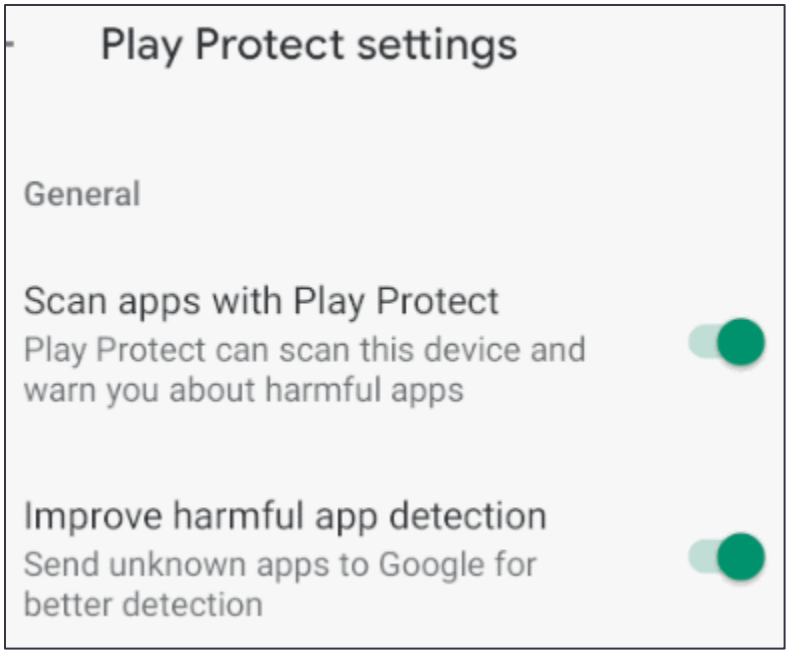
- In the top left, tap the **back arrow** until you are back to the *Settings* screen. Then, tap **Privacy**.[118]
- Tap **Autofill service from Google**, if you want your device to automatically fill in personal info, addresses, and passwords for you. If you previously enabled this and now want to disable it, I will tell you how in the *System* section.[119]
- Go back to the **Privacy** screen, then tap **Advanced**, then **Activity controls**. I recommend that you toggle **off** as many as possible, to reduce the amount of data Google collects about you. I cover these controls at the following **URL**.[120]
- Go back to the **Privacy** screen, then tap **Ads**. Toggle **on** *Opt out of Ads Personalization* to reduce the amount of data Google collects about you.
- Go back to the **Privacy** screen, then tap **Usage & diagnostics**. I like to share data that helps make software and services better if my data is anonymized. If you prefer, you can toggle **Off**.

9.6.5.1 Location

- In the top left, tap the **back arrow** until you are back to the *Settings* screen. Then, tap **Location**.[121]
- If you do not want to use the location at all, you can toggle **off** *Use location*. Note that location must be on for *Find My Device* to work (which lets you remotely find, lock, and wipe/erase your device).[122]
- Tap **Wi-Fi and Bluetooth scanning**. I recommend toggling these **off** unless you truly need exact locating. If you toggle these on your device can use Wi-Fi and Bluetooth signals for location, even when you have turned off Wi-Fi and Bluetooth.[123]

9.6.5.2 Android Security

- In the top left, tap the **back arrow** until you are back to the *Settings* screen. Then, tap **Security**.[124]
- Tap **Google Play Protect**, then the **gear icon** in the top right. Toggle **on** *Scan apps with Play Protect* and *Improve harmful app detection*.[125]



- Go back to the **Security** screen, then tap **Find My Device**. It is recommended toggling this **on**. It allows you to remotely find, lock, and wipe/erase your device if it becomes broken, lost, or stolen.
- Go back to the **Security** screen, then tap **Security update**, if you see it. If it shows an available update, **install it**.
- Go back to the **Security** screen, then tap **Screen lock**. Setting a password is best, but because it is annoying to type a password on a mobile device, consider **setting a pattern or PIN**. Ensure the pattern is complex, and the PIN is at least 6 digits (the longer, the better).
- Go back to the **Security** screen, then tap **Fingerprint**. You can choose to use your fingerprint along with another screen lock method.
- Go back to the **Security** screen, then tap **Advanced**, then **Encryption & credentials**. If you do not see **Encrypted** under **Encrypt phone**, then **tap** it to enable encryption. Encrypting your device is one of the best things you can do to secure it, because it means that if someone steals your device, they will not be able to see or copy your data off the device.

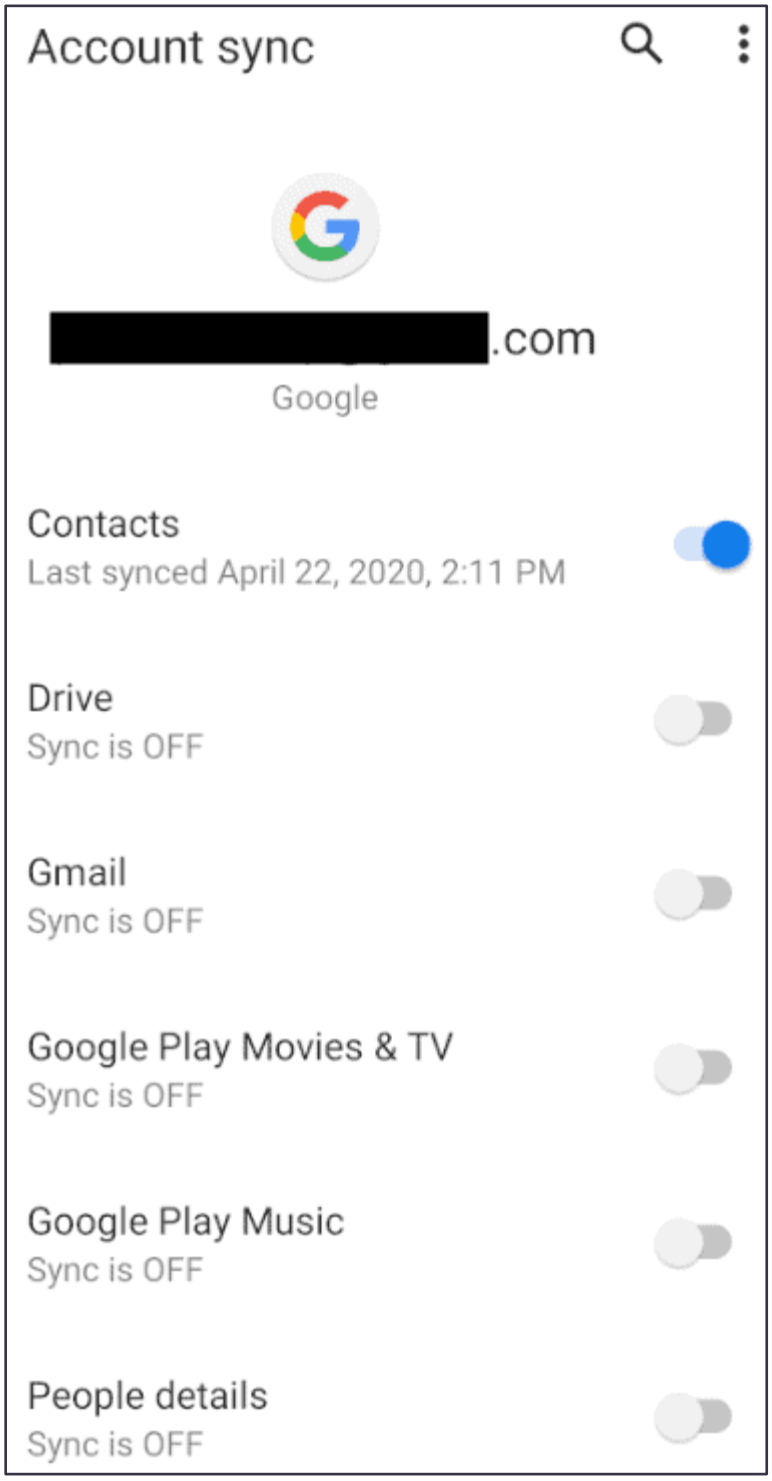
9.6.5.3 Text (SMS) Message Security

- Text (SMS) messages are not secure. If you are communicating about anything sensitive or confidential, you should consider a secure, private messaging app.[126]

9.6.5.4 Accounts

- In the top left, tap the **back arrow** until you are back to the *Settings* screen. Then, tap **Accounts**.
- Android is meant to be used with a Google account. If you sign into a Google account, you will have many more options. However, you can use an Android device without a Google account. Another choice is to create a separate Google account that you use just for Android, and do not use it for anything else.
- You can toggle **Automatically synchronize data** if you want apps to automatically synchronize with accounts. If you toggle it off, you can still manually synchronize accounts.

- Tap an account, then tap **Account sync** to customize what is synchronized. Toggle off any items that you do not need to be synchronized to your device.



9.6.5.5 Android Anti-Malware

- It is always recommended that you use antivirus software to protect your Android device.

- One choice is to manually scan weekly (run an ***on-demand scan***), rather than having an anti-malware app run constantly in the background (sometimes called ***real-time scanning***).

9.6.6 Android Private DNS Overview

Google has brought DNS over TLS support to Android by introducing the Private DNS feature.[127] It is available in Android 9 (Pie) and higher, and encrypts all DNS traffic on the phone, including from apps.

The feature is enabled by default and uses a secure channel to connect to the DNS server if the server supports it. But if your ISP or cell service provider's DNS does not have encrypted DNS support, or you are simply not sure about it, you can use a third-party secure DNS server using the Private DNS feature.[128]

9.6.7 Using Private DNS

- To manage Private DNS options, **swipe down** from the top of your device to access the notification shade and tap the **gear icon**. This will take you to device settings. You can also reach the settings page from the **apps drawer**.[129]
- Once you are in the settings, tap **"Network & Internet."** Depending on your device, this might have a slightly different name, like **"Connections."**
- Now tap on **"Private DNS"** to manage the feature. If you do not immediately see the **"Private DNS"** option, you may have to tap on **"More Connection Settings"** or **"Advanced"**.
- You will get three options: **Off**, **Automatic**, and **Private DNS provider hostname**. You can select **"Off"** to stop using DNS over TLS, **"Automatic"** to use encrypted DNS when available, or write the hostname of a **"Private DNS provider"** to use encrypted DNS from that provider. Remember, rather than DNS server IPs, you need a hostname.
- Once done, tap on **"Save"** to apply the changes.

9.6.8 Testing For DNS

You can confirm whether your internet provider supports TLS protocol for DNS encryption by using Avast-owned company at the following **URL** as it shows whether your ISP's DNS is TLS enabled or not.

9.7 Google Account Settings

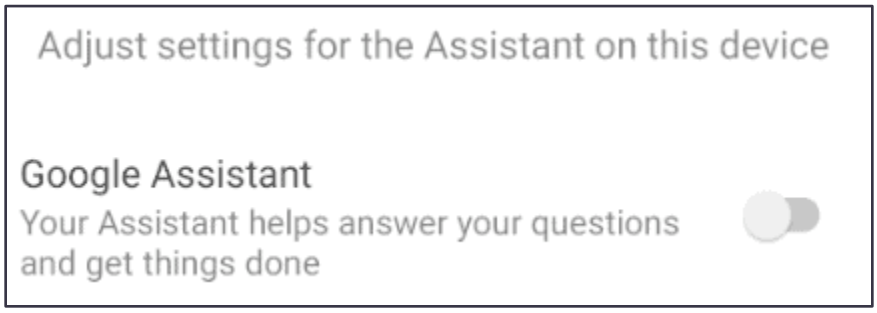
- In the top left, tap the **back arrow** until you are back to the *Settings* screen. Then, tap **Google**.
- Tap **Account services**, then **Connected apps**. You will see the apps and devices connected to your Google account. If any should be disconnected, tap them, and click **Disconnect**.
- In the top left, tap the **back arrow** until you are back to the **Account services** screen. Then, tap **Search, Assistant & Voice**, then **Google Assistant**. Google Assistant is, well, Google's digital assistant, the equivalent of Amazon's Alexa and Apple's Siri. To work, Google Assistant sends a lot of data about what you say, type, and do to Google. If you do not want to use it, tap the **Assistant** tab, and scroll down to **Assistant devices**. Tap your device. Then, toggle **off Google Assistant**.
- Anyone who is near your Google speaker or display device can request information from it, and if you have given your device access to your calendars, Gmail or other personal information, people may be able to ask your device about that information, depending on your **Personal Results Settings** and **Voice Match Settings.**[130] Google employees and trusted third parties can also access your conversation history in line with Google's **Privacy Policy.**[131]

9.7.1 Google Location Services

Location History is a Google Account–level setting that saves where a user goes with every mobile device.[132] To disable this feature, follow the steps below:

- Go to **Settings** in your Google account.
- Choose **"Data & Privacy"** in the left tab.
- Scroll down to the **History Settings** menu.
- Click on the **Location History** settings.
- Toggle **Location History** off.

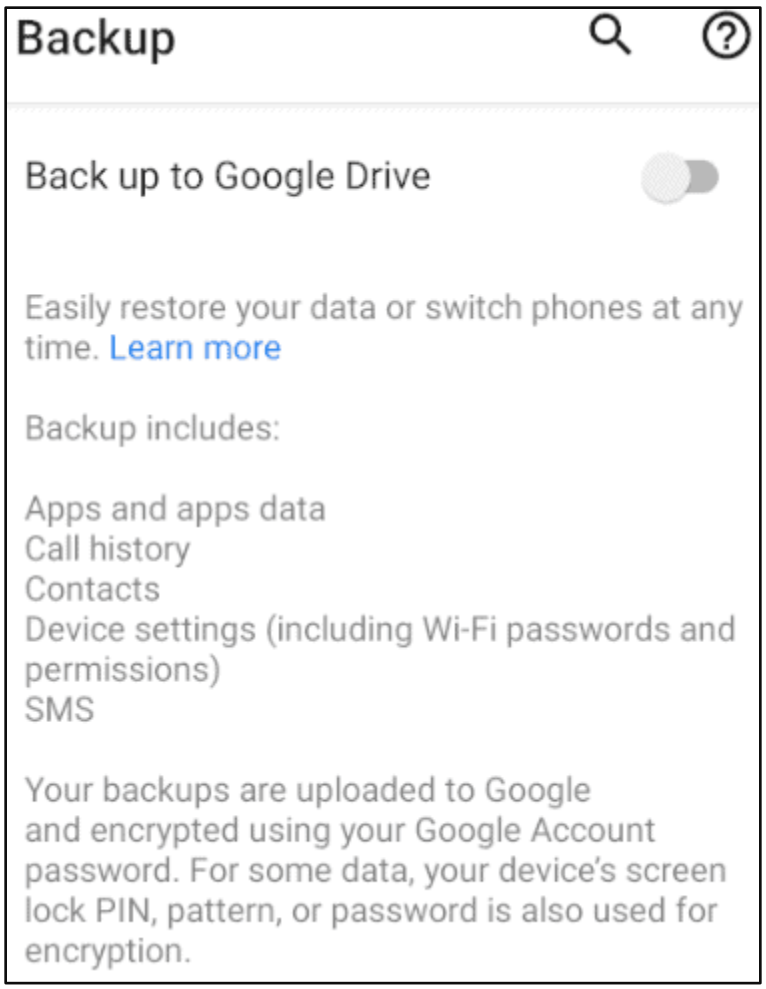
9.7.2 Google Assistant



- If you want to use Google Assistant, go back to the **Account services > Search, Assistant & Voice** screen and configure the settings in **Google Assistant** and **Voice**.
- If your child will be using this device, you can go back to the *Google* screen and tap **Parental controls** to set up **Google Family Link**. It lets you control content, apps, and screen time.[133]

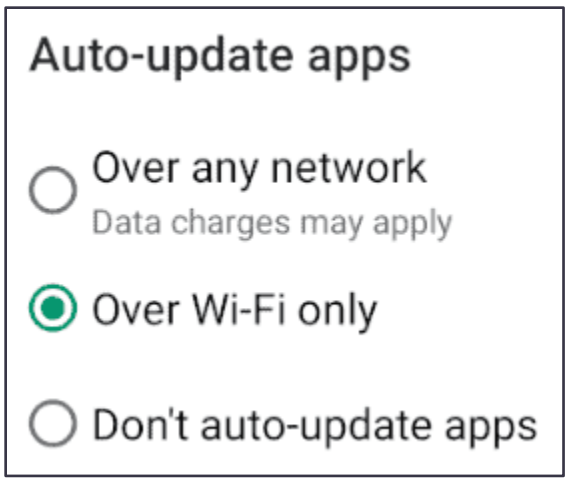
9.7.3 Google System

- In the top left, tap the **back arrow** until you are back to the **Settings** screen. Then, tap **System**.
- If you previously enabled **Autofill service from Google** (to automatically fill in personal info, addresses, and passwords) and now want to disable it, tap **Languages & input**, then **Advanced**, then **Autofill service**, then **Autofill service**. Then, select **None**.
- Go back to the **System** screen, then tap **Backup**. Toggle on **Back up to Google Drive** unless you will be using a different backup service. If you are running Android 9 ("Pie") or later, Google cannot see your backup data.
- If your backups are uploaded in Google, they are encrypted using your Google Account password. For some data, your phone's screen lock PIN, pattern, or password is also used for encryption.
- This decryption key is encrypted using the user's lock screen PIN/pattern/passcode, which is not known by Google. By design, this means that no one (including Google) can access a user's backed-up application data without specifically knowing their passcode.



9.7.4 Updating Google Apps

- Because app updates often fix security vulnerabilities, you should **install** them as soon as they are available.[134]
- Open the **Google Play** app, then tap the **menu** (hamburger icon, three horizontal lines in the top left), then tap **Settings**, then **Notifications**. Toggle **on Updates.**
- Tap the **back arrow** in the top right to go back to **Settings**, then tap **Auto-update apps**. Set it to **Over Wi-Fi only**. If you rarely connect to Wi-Fi, set it to **Over any network**.
- Whenever your device shows that updates are waiting to be installed, **install** them.



9.7.5 Google Play Data Safety Section

Google designed the Data safety section to allow developers to clearly mark what data is being collected and for what purpose it is being used. Users can also see whether the app needs this data to function or if this data collection is optional. With the new Data Safety section, Google requires the app developers to provide users with information like how their data is collected by the apps.[135]

The section primarily shows the information on if an app is collecting the user data, for what purpose, and if the app is following Google Play's Families Policy. It also answers the question of whether the user data is shared with third parties. It also highlights the app developers' safety measures taken to protect the user data.[136]

The Google Play Data Safety Section gives users data on the following issues:

- Whether the developer is collecting data and for what purpose.
- Whether the developer is sharing data with third parties.
- The app's security practices, like encryption of data in transit and whether users can ask for data to be removed.
- Whether a qualifying app has committed to following **Google Play's Families Policy** to better protect children in the Play store.[137]
- Whether the developer has confirmed their security practices against a global security standard, **more specifically, the MASVS**.[138]

9.7.6 Google Voice Recordings

Google has **suspended human review** of audio recordings. However, if you are still cautious, there are two ways to turn off the voice activity.

- On your Mobile Phone, you can also open the **Google Home** mobile app.
- Select your **Profile Icon** > **My Activity** > **Saving Activity**.
- Toggle **Include Audio Recordings** on or off.
- On your PC, go to **URL** and click the **Settings Bars** in the top left.
- Click **Activity Controls.**

- Next, uncheck the box that says **Include Audio Recordings** to prevent Google from linking your voice recordings with your account.

To delete your voice command history:

- Go to **URL > Data and Personalization** > **Web & App Activity** > **Manage Activity >** Tap the **three stacked dots** menu at the top of the screen
- Select **Delete Activity By** and choose from the options -- all time, last hour, last day, etc.
- Tap **Delete** to confirm.
- You can also tell Google to delete your voice command history. Just say, "Hey, Google, delete everything I just said."

9.8 Mobile Two-Factor Authentication

- If you do not have two-factor authentication (2FA) enabled yet on your iPhone, consider doing so. This adds another layer of security to your logins by requiring more than just your password.[139]
- These codes often arrive via text or email, though you can get 2FA codes through an app instead. Here is how to enable that feature:

9.8.1 iPhone Two-Factor Authentication

Here is how to enable that feature on an iPhone:

- Go to **Settings** > **[your name]** > **Password & Security** and tap **Turn on Two-Factor Authentication**.
- Tap **Continue**, then enter the phone number where you want to receive the verification codes.
- Tap **Next** and enter the code.

9.8.2 Android Two-Factor Authentication

Here is how to enable that feature on an Android:

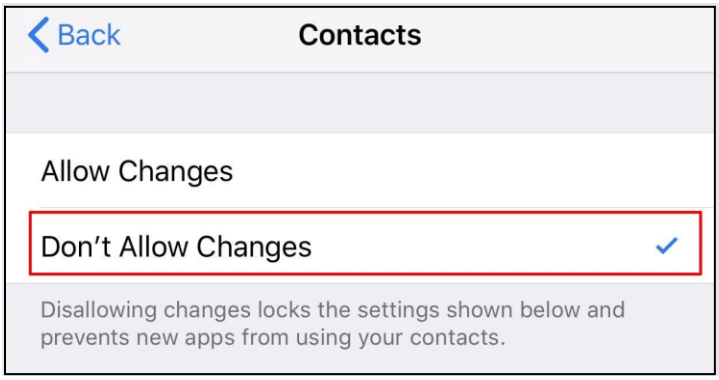
- Open your Google Account and select **Security**.
- Select **2-Step Verification** (under Signing into Google) and then **Get started**.
- Now pick a method for verification: Google prompts, security keys, Google Authenticator or similar apps, or a verification code sent to your phone via text or call.

9.9 Stop Contacts From Syncing To Mobile Apps

9.9.1 iPhone Settings

- Go to **Settings, Screen Time**, and then **Content & Privacy Restrictions** (as shown in the graphic).

- Then, Enable **Content & Privacy Restrictions**.
- Scroll down to the Privacy section and tap on **Contacts.** Tap **Do not Allow Changes** to lock the settings. Your iPhone's contacts are now locked down from Apps.



9.9.2 Android Settings

Steps may vary depending on which Android Mobile Phone you use, but generally:

- Open the **Settings** app.
- Tap the **Apps & notifications** choice.
- Tap the app you want to examine.
- Tap **Permissions** to see everything the app can access.
- To turn **off** permission, tap on it. You might need to tap a confirmation box here as well.

9.10 Securing Your Personal Email Address

Create unique disposable email addresses for different online accounts. ***It is also highly recommended that you create a separate email address when opting out of your Digital Exhaust.***

- This can be read about at this **URL**.

9.10.1 Checking URLs in Emails

Hyperlinks in email can often connect to a web domain different from what they appear to be. Some links may display a recognizable domain name, but, in fact, direct the user to a different, malicious domain. Threat actors also use international character sets or misspellings to create malicious domains that is those of well-known brands.[140]

Users are encouraged to always review link contents by hovering the mouse pointer over the link to see if the actual link is different from the displayed link. The resources below will also aid users in making informed decisions when receiving links in emails.

9.10.1.1 Checking Shortened URLs

One clue that a link in email may be dangerous is that the URL seems too short. While link-shortening services such are popular and common tools for creating shorter links, threat actors also use link shortening to conceal their links' true destinations.[141] The following websites will help users in determining the legitimacy of shortened URLs.

Service	Website
CheckShortURL	https://checkshorturl.com/
UnShorten.IT	https://unshorten.it/

9.10.1.2 URL Scanning Websites

URL scanners are websites and that let you enter the URL of a suspicious link and check it for safety.[142] The following websites will help users in determining the legitimacy of shortened URLs.

Service	Website
VirusTotal	https://www.virustotal.com/gui/home/url
Norton SafeWeb	https://safeweb.norton.com/
URLVoid	https://www.urlvoid.com/
PhishTank	https://www.phishtank.com/

10 PRIMARY DATA BROKERS

Data brokers collect and sell data about consumers.[143] [144] They do not have a direct relationship with anyone they collect about, but they do sell data to other parties, like companies or individual marketers, for their commercial purposes.[145, 146, 147, 148, 149, 150] Primary data brokers sell data to other data brokers.[151]

Primary Data Broker	Opt Out Method
Acxiom	https://isapps.acxiom.com/optout/optout.aspx
CoreLogic	https://www.corelogic.com/privacy-policy/ It is recommended you contact them via the email **privacy@corelogic.com** and you can provide them with documentation to opt out available at URL https://www.corelogic.com/downloadable-docs/teletrack-out-opt-form.pdf
Oracle Data Cloud	https://datacloudoptout.oracle.com/optout/
Epsilon	1. Email optout@epsilon.com; or, 2. Call 1-888-780-3869; or, 3. Send mail to Epsilon, P.O. Box 1478, Broomfield, CO 80036
AddThis	https://www.addthis.com/privacy/email-opt-out
Data and Marketing Choice	https://dmachoice.thedma.org/register.php (Please note that DMA is now charging a $2 fee to register online. If you do not wish to pay $2, you can use the following URL https://dmachoice.thedma.org/prefill_mailin_registration.php to fill out a form and mail your request into DMA.)
Direct Mail	http://www.directmail.com/mail_preference/
E-Bureau	http://www.ebureau.com/privacy-center/opt-out for Opting Out will now route you to TransUnion's Opt Out link. It should be noted that older Opt Out guidance lists Opting Out of E-Bureau so simply Opt Out through TransUnion.
Experian	https://www.experian.com/privacy/opting_out.html
Opt Out Prescreen	https://www.optoutprescreen.com/selection
TowerData	https://instantdata.towerdata.com/optout/
TransUnion Consumer	https://www.transunion.com/customer-support/marketing-offers-opt-out

11 PEOPLE SEARCH SITES

People search sites enable the public to search names and other personally identifiable information.[152, 153, 154, 155] Returns from these searches include property addresses, points of contact, family members, aliases, and more associated with the searched information with varying degrees of accuracy.

11.1 People Search Sites Opt Out List

People Search Site	Opt Out Method
Addresses	https://www.intelius.com/opt-out/submit/
Archives	http://www.archives.com/?_act=Optout
BeenVerified	https://www.beenverified.com/f/optout/search
Cubib	https://cubib.com/optout.php
FamilyTreeNow	https://www.familytreenow.com/optout
FastPeopleSearch	https://www.fastpeoplesearch.com/removal
Instant Checkmate	https://www.instantcheckmate.com/opt-out/
Intelius	https://www.intelius.com/optout
Lexis Nexis	https://www.lexisnexis.com/en-us/privacy/for-consumers/opt-out-of-lexisnexis.page?
Peek You	https://www.peekyou.com/about/contact/optout/
People Finders	https://www.peoplefinders.com/opt-out
People Smart	https://www.peoplesmart.com/optout-go
People Wiz	https://www.peoplewhiz.com/remove-my-info
Pipl	https://pipl.com/help/remove/
Radaris	https://radaris.com/ng/page/removal-officer
Social Catfish	https://socialcatfish.com/opt-out/
Spokeo	https://www.spokeo.com/optout
SpyFly	https://www.spyfly.com/help-center/remove-info
ThatsThem	https://thatsthem.com/optout
TruePeopleSearch	https://www.truepeoplesearch.com/removal
USA People Search	https://www.usa-people-search.com/manage/
White Pages	https://www.whitepages.com/data-policy
USPhoneBook	http://www.usphonebook.com/opt-out

11.2 Removing PII On Web Search Engines

11.2.1 URL Removal Of PII From Google Search

Google may remove personally identifiable information (PII) that has potential to create significant risks of identity theft, financial fraud, harmful direct contact, or other specific harms.[156] This includes doxing, which is when your contact info is shared in a malicious way. This article is intended to support you through the process to request removal of such content from Google search results.[157]

Google will evaluate each request based on the criteria listed below and evaluate the content for public interest. As a result of this review, Google may:

- Remove the provided URL(s) for all queries,
- Remove the URL(s) for only queries including your name, or
- In some circumstances, deny your request.

11.2.1.1 Google Requirements To Remove PII

For Google to consider the content for removal, it must pertain to the following types of information:

- Confidential government identification (ID) numbers like U.S. Social Security Number, Argentine Single Tax Identification Number, Brazil Cadastro de pessoas Físicas, Korea Resident Registration Number, China Resident Identity Card, etc.
- Bank account numbers
- Credit card numbers
- Images of handwritten signatures
- Images of ID docs
- Highly personal, restricted, and official records, like medical records
- Personal contact info (physical addresses, phone numbers, and email addresses)
- Confidential login credentials

11.2.1.2 Google Requirements To Remove Doxing Content

For Google to consider the content for removal, it must meet both requirements:

- Your contact info is present.

There is the presence of:

- Explicit or implicit threats, or
- Explicit or implicit calls to action for others to harm or harass.

11.2.1.3 Request To Remove Select Personal Info From Google Search

You or your authorized representative can send a request to remove links to the content from Google search results. Any authorized representative will need to explain how they have the authority to act on your behalf. Google only reviews the URLs that you or your authorized representative sends in the form. To start a removal request with Google you can navigate to the following **URL**.

11.2.1.4 What Happens After You Submit The Removal Request?

You get an automated email confirmation. This confirms Google received the request. Google reviews your request. Each request is evaluated on factors including the requirements above. Google gathers more info, if needed. In some cases, Google may ask you for more information. If the request does not have enough information for Google to evaluate, like missing URLs, Google will share specific instructions and ask you to resubmit the request.

You get a notification of any action taken. If the sent URLs are found to be within the scope of our policy, either the URLs will be removed for all queries or the URLs will be removed only from search results in which the query includes the complainant's name, or other provided identifiers, such as aliases. If the request does not meet the requirements for removal, Google will also include a brief explanation. If your request is denied and later you have other materials to support your case, you can re-submit your request.

11.2.1.5 Removal Of Outdated Google Content

If the content no longer appears on the webpage but appears in Google search results or as a cached page, request removal with the **Outdated URL removal tool**.

11.2.2 Bing Content Removal Reporting

The **Content Removal Tool** allows you to let Bing know about two types of outdated content in their web results:

- Pages that appear in Bing's web search results that are broken links (404 - Not Found).
- Pages that appear in Bing's web search results that have outdated content in the cached version of the page.

11.2.2.1 Removing a Broken Link (Page Removal)

When a page has been removed from a website it will eventually drop out of Bing's search index as Bing will re-crawl the page and find it is gone. However, this re-crawl process can take time. The Content Removal tool allows you to let Bing know of the fact that the URL of the page is broken *(404 - Not Found)*.

If you send a page removal request, Bing will check whether the page is in fact no longer live on the web, and if that is the case, Bing will speed up removing the URL from their search results. If, however, the URL points to a page that is still live on the web, you are given the choice to remove outdated cached content instead. If Bing is unable to decide either (for example, because Bing cannot connect to the server on which the page resides), you will not be able to send a page removal or outdated cache removal request at this moment in time.

11.2.2.2 Steps to Submit a Page Removal Request

You can send a page removal request for a page that is no longer live on the web (404) by doing the following:

- Go to **URL** and sign in with the account you use for **Bing Webmaster Tools.**
- In the **Content URL** input box, enter the **exact URL** you found in the Bing web results (for example, by using Copy Shortcut/Copy Link Address functionality in your browser).
- In the **Removal Type** drop-down menu select **Page Removal.**
- Click **Submit.**

When you click send, Bing will run a check whether the page is no longer available on the web. If that is the case, Bing will send the request and add it the **Submission History** table. However, if Bing detects that the page is still live on the web Bing will prompt that you can only send an outdated cache removal (see steps below).

11.2.2.3 Removing Outdated Cache (Outdated Cache Removal)

When a page is still live on the web, the Bing crawler *(Bingbot)* will revisit it in regular intervals to update the content Bing's index and store a copy in the Bing cache. However, changes can take time to be reflected in the index and the cached page. You can let Bing know about outdated cache by supplying the URL and a piece of text from the outdated cached page that is no longer present on the page that is live on the web.

11.2.2.4 Steps to Submit An Outdated Cache Removal Request

You can send an outdated cache removal request for a page that is live on the web *(HTTP status code 200)* and for which Bing still has old and outdated content in their cache by doing the following:

- Go to **URL** and sign in with the account you use for **Bing Webmaster Tools** (formerly known as Windows Live ID).
- In the **Content URL** input box, enter the **exact URL** you found in the Bing web results (for example, by using Copy Shortcut/Copy Link Address functionality in your browser).
- In the **Removal Type** drop-down menu, select **Outdated Cache Removal.**
- In the **Cached Page Text**, enter the text that still appears on the cached page that no longer appears on the page that is live on the web.
- Click **Submit.**

Bing will now check whether the page no longer holds the words that you have entered. If Bing has established that, your request will be added to the Submission History table below, showing you the date, Content URL, Removal Type and Status, along with the HTTP Status Code we received from the server.

The Submission History table will show you the most recent submissions that were made for the account with which you are logged in. Since this is a history table of the requests you made and their status, you cannot remove or edit individual items afterwards.[158]

12 LOCATION DATA BROKERS

Location data is geographical information about a specific device's whereabouts associated to a time identifier. This device data is assumed to correlate to a person – a device identifier then acts as a pseudonym to separate the person's identity from the insights generated from the data. Location data is often aggregated to supply significant scale insights into audience movement.[159]

Apple and Google both have policies for companies selling location data.

Apple's policy requires apps to show what data they are collecting from people and how it can be used and to get consent from users before sharing their data.[160] However, it does not require apps to show exactly who they are selling data to, and many apps simply say that they share data with partners. For location data specifically, once the user has granted permissions, Apple's policy notes that people are subject to apps' privacy policy and practices, which can include selling their data.[161]

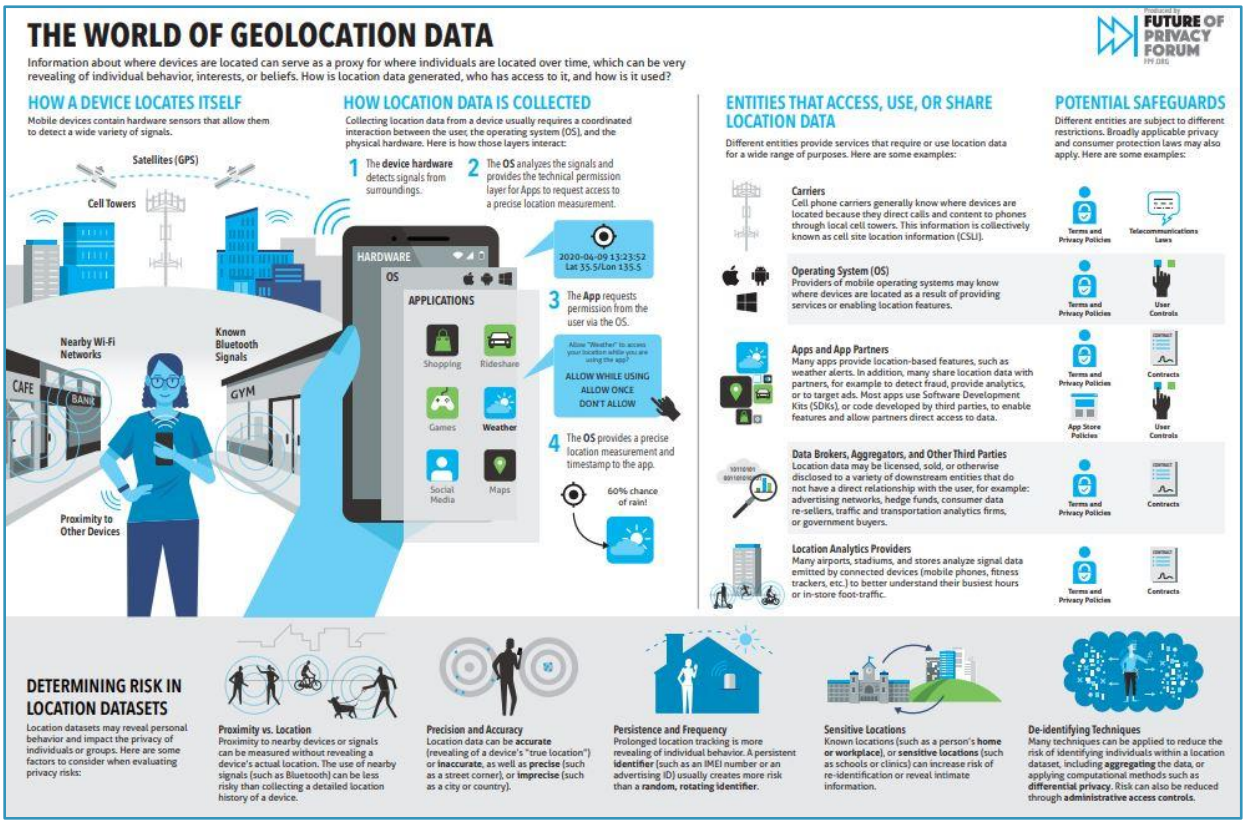
Google's states developers cannot sell personal and sensitive user data, which includes device location. The company also needs disclosure, telling developers that they "must be transparent in how you handle user data."[162]

12.1 Geolocation Data Overview

Information about where devices are found can serve as a proxy for where individuals are found over time[163], which can be very revealing of an individual's behavior[164], interests, or beliefs[165].

- Mobile devices, from smart phones to tablets to fitness trackers, have become intertwined in many people's lives over the last decade, supplying many benefits and becoming almost indispensable.[166]
- However, the benefits and convenience can come at a cost.[167]
- Mobile devices store and share valuable location data by design.[168]
- This data can reveal details about the number of users in a location, user and supply movements, daily routines and can expose otherwise unknown associations between users and locations.[169]

The following graphic give you an overview of how location data is generated, who has access to it, and how is it used.



12.2 Location Data Brokers Opt Out List

Company	Website	Opt Out Link	Privacy Policy

1010Data	https://www.1010data.com/	privacy@1010data.com	https://www.1010data.com/privacy-policy/
Acxiom	http://www.acxiom.com/	consumeradvo@acxiom.com	https://www.acxiom.com/about-us/privacy/highlights-for-us-products-privacy-policy/
AdSquare	https://www.adsquare.com/	https://adsquare.com/privacy-policy-and-opt-out/	https://www.adsquare.com/privacy/
ADVAN	https://advanresearch.com/	privacy@advanresearch.com	https://advanresearch.com/privacy_policy
Airsage	https://www.airsage.com/	support@airsage.com	https://www.airsage.com/airsage-privacy-policy/
Amass Insights	https://amassinsights.com/#/	info@amassinsights.com.	https://amassinsights.com/#/privacy-policy
Alqami	https://www.alqami.com/	enquiries@alqami.com	https://www.alqami.com/privacy-policy
Amazon AWS Data Exchange	https://aws.amazon.com/data-exchange/	No email: https://console.aws.amazon.com/support/home	https://aws.amazon.com/privacy/
Anomaly 6	https://www.anomalysix.com/	N/A	N/A
Babel Street	http://babelstreet.com/	privacy@babelstreet.com	https://babelstreet.com/privacy-policy
Blis	https://blis.com/	privacy@blis.com	https://blis.com/privacy-centre/
Complementics	https://www.complementics.com/	http://www.complementics.com/opt-out	http://www.complementics.com/optout-donotsell
Cuebiq	http://www.cuebiq.com/	https://www.cuebiq.com/privacy-request/	https://www.cuebiq.com/privacy-request/
Datarade	https://datarade.ai/	privacy@datarade.ai	https://about.datarade.ai/legal/privacy-policy
Foursquare	https://foursquare.com/	https://foursquare.com/data-requests/	https://foursquare.com/legal/privacy
Gimbal	https://gimbal.com/	https://gimbal.com/opt-out/	https://gimbal.com/legal/#privacy
Gravy Analytics	https://gravyanalytics.com/	https://gravyanalytics.com/opt-out-do-not-sell/	https://gravyanalytics.com/request-your-information/
GroundTruth	http://www.groundtruth.com/	requests@groundtruth.com	https://www.groundtruth.com/privacy-policy/
Huq Industries	https://huq.io/	hello@huq.io	https://huq.io/privacy-policy/#a
InMarket / NinthDecimal	http://www.inmarket.com/	https://inmarket.com/opt-out/	https://inmarket.com/request-my-information/
Irys	https://irys.us/	privacy@irys.us	https://irys.us/privacy-policy
Kochava Collective	https://www.kochava.com/	privacy@kochava.com.	https://www.kochava.com/support-privacy/?int-link=menu-data-privacy
Lifesight	https://www.lifesight.io/	https://www.lifesight.io/do-not-sell-my-personal-info/	https://www.lifesight.io/privacy-policy-eng/
Mobilewalla	http://www.mobilewalla.com/	https://www.mobilewalla.com/ccpa-opt-out-request	https://www.mobilewalla.com/business-services-privacy-policy
Narrative	https://www.narrative.io/	privacy@narrative.io	https://www.narrative.io/privacy-policy
Near	https://near.co/	https://near.wirewheel.io/privacy-	https://near.co/privacy/

		page/614c395a6a9fca00143453ae	
Onemata	https://onemata.com/	https://www.onemata.com/do-not-sell-my-personal-info	https://www.onemata.com/privacy-policy
Oracle	https://www.oracle.com/	No email. Use form: https://www.oracle.com/legal/data-privacy-inquiry-form.html	https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html
Phunware	https://www.phunware.com/data/customer-data-platform/	https://www.phunware.com/privacy/optout/	https://www.phunware.com/privacy/optout/
PlaceIQ	http://www.placeiq.com/	privacy@placeiq.com	https://www.placeiq.com/privacy/
Placer.ai	https://www.placer.ai/	privacy@placer.ai	https://www.placer.ai/privacy-policy/sdk-user-privacy-policy/
Predicio	http://www.predic.io/	http://www.predic.io/opt-out	http://www.predic.io/privacy-us
Predik Data-Driven	https://predikdata.com/en/home/	info@predikdata.com	https://predikdata.com/en/predik-data-driven-privacy-policy/
Quadrant	https://www.quadrant.io/	https://www.quadrant.io/do-not-sell	https://www.quadrant.io/data-requests
QueXopa	https://quexopa.io/	info@quexopa.io	https://quexopa.io/privacy-policy/
Reveal Mobile	http://www.revealmobile.com/	https://revealmobile.com/ccpa/	https://revealmobile.com/privacy/
SafeGraph	http://www.safegraph.com/	privacy@safegraph.com	https://www.safegraph.com/privacy-policy
Snowflake	https://www.snowflake.com/data-marketplace/	privacy@snowflake.com	https://www.snowflake.com/privacy-policy/
start.io	http://www.start.io/	support@start.io	https://www.start.io/policy/privacy-policy/
Stirista	http://www.stirista.com/	privacy.officer@stirista.com	https://www.stirista.com/privacy-policy/
Tamoco	http://www.tamoco.com/	privacy@tamo.co	https://www.tamoco.com/privacy-policy
THASOS	http://thasosgroup.com/	http://thasosgroup.com/privacy-policy/	http://thasosgroup.com/privacy-policy/
Unacast	http://www.unacast.com/	https://www.unacast.com/opt-out	https://www.unacast.com/privacy
Venntel	https://www.venntel.com/	https://www.venntel.com/opt-out?hsLang=en	https://www.venntel.com/privacy-policy?hsLang=en
Venpath	https://www.venpath.net/	https://www.venpath.net/legal/opt-out	https://www.venpath.net/legal/privacy-policy
Veraset	https://www.veraset.com/	https://www.veraset.com/do-not-sell-my-personal-information/	https://www.veraset.com/privacy-policy/
X-Mode (Outlogic)	https://xmode.io/	https://xmode.io/optout-donotsell/	

13 TELEPHONE NUMBERS AND TEXT MESSAGES

Our cell phone numbers are a single point of failure as we use them to sign up to sites and services, log into an apps, reset our account if we forget our passwords as well as for two-factor authentication to securely login to our accounts. Just think of every site and service that has your phone number. That is why you need to protect your phone number. With your phone number, a threat actor can start hijacking your accounts and spoof your identity.[170]

13.1 TELEPHONE NUMBER SAFETY RECOMMENDATIONS

There are many ways your phone number is exposed, and you might not be aware how many ways your data is shared online.[171]

- Your phone number could be linked to your social media or other online account. Check the settings on your social media profiles to make sure personal information like your phone number is made private.
- You overshared your phone number. You may have entered your information for a free trial, contest, or other online form, which potentially opened you up to receiving unwanted calls.
- You accepted the terms and conditions without reading the entire Terms of Service. Make sure to read the terms and conditions to see exactly where your information is being shared.
- You supplied your phone number for a product you bought. You also may supply your phone number to retailers for loyalty points or discounts.
- Your phone number was part of a data breach, making you easily accessible to scammers. Companies involved in data breaches must show what information was exposed. If you are unsure whether your information was included, call the company directly and inquire.

13.1.1 Block Unwanted Robocalls

The major wireless providers offer various tools and solutions that you can engage or may be built into your device to block or flag calls.[172]

- **AT&T Call Protect**[173]
- **Verizon Call Filter**[174]
- **T-Mobile Scam ID, Scam Block, Name ID**[175]
- **U.S. Cellular Call Guardian**[176]

13.1.1.1 Use Built In Mobile Phone Features

Use features built into your phone to block unwanted calls. To learn more, check out guides for **iOS** and **Android** or visit your device manufacturer's website.

13.1.1.2 Do-Not-Call Registry

Adding your number to the **Do-Not-Call Registry** prohibits telemarketers from calling your registered number.[177]

13.1.1.3 Reporting Robocalls to the FCC or FTC

Users can file a complaint with the **FCC** or **FTC** if you receive robocalls you believe to be spam.[178]

13.1.1.4 Precautions With Unknown Callers

Do not engage with suspicious robocalls. Do not give out personally identifiable information or send money to a third party without verifying the authenticity of the caller. You can double check the authenticity of the caller by looking up their phone number on their website or in a phone book and calling them directly.

13.2 Block Unwanted Calls

13.2.1 Your Personal Telephone Number

Your personal telephone number is one of your biggest digital exhaust personal vulnerabilities.[179] [180]You can decrease this vulnerability by setting up extra security for the phone. [181]

- If you switch your phone number, often, recycled numbers allow new customers access to old customer information, opening opportunities for a variety of potentially exploitative encounters.[182]
- Create a security code and/or obfuscate the true number by creating a separate forwarding number. Read about this at the following **URL**.[183]

13.2.2 iPhone: How To Block A Number

There are multiple methods of how to block a number on iPhone devices. Before following the steps below, make sure your iPhone is updated.

13.2.2.1 Via Your Call History

- Go to your **Phone** icon/app.
- Click on the **blue ?** symbol next to the restricted call.
- Choose **Block this caller** to block the specific restricted call.

13.2.2.2 Use Do Not Disturb

- Go to **Settings** > **Do Not Disturb**.
- Scroll down to **Allow Call From** and click on that.
- Choose who you want to **accept** calls from, such as your **Favorites** or **All Contacts**.
- On the **Do Not Disturb** page, make sure your other settings are set the way you want them.
- Turn **on** the **Do Not Disturb button** at the top of the page.

13.2.3 Android: How To Block A Number

- Go to your **Phone** icon.
- Click on the **restricted** call and then the **?** symbol (may also say **Details***).*
- Choose **Block Number** at the bottom of your screen.[184]

13.2.3.1 Set up a Personal Telephone Number Code

Carrier	Instruction
AT&T	https://www.att.com/esupport/article.html#!/wireless/KM1051397?gsi=Ks1FJro
Sprint	https://www.sprint.com/en/support/solutions/account-and-billing/learn-more-about-your-account-pin.html
T-Mobile	https://support.t-mobile.com/docs/DOC-37477
Verizon	https://www.verizonwireless.com/support/account-pin-faqs/

13.2.3.2 Set up a Separate Forwarding Telephone Number

Platform	Technology	Privacy Advice
Apple	Google Voice	https://itunes.apple.com/us/app/google-voice/id318698524?mt=8
	My Sudo	https://mysudo.com
	Others	https://www.makeuseof.com/tag/5-apps-getting-temporary-burner-phone-number/
Android	Google Voice	https://play.google.com/store/apps/details?id=com.google.android.apps.googlevoice&hl=en_US
	Others	https://www.makeuseof.com/tag/5-apps-getting-temporary-burner-phone-number/

13.3 Block Unwanted Text Messages

If you get a text message that you were not expecting and it asks you to give some personal information, do not click on any links. Legitimate companies will not ask for information about your account by text.

If you think the message might be real, contact the company using a phone number or website you know is real. Not the information in the text message.

There are many ways you can filter unwanted text messages or stop them before they reach you.

13.3.1 On Your Phone

Your phone may have a choice to filter and block messages from unknown senders or spam. To enable these features, see the links below:

13.3.1.1 Filter, Block Messages On iPhone

You can block phone numbers, contacts, and emails on your device. You can also filter iMessages from unknown senders and report iMessages that look like spam or junk. **URL** [185]

13.3.1.2 Filter, Block Messages On Android

Some of these steps only work on Android 6.0 and up. **URL** [186]

If you have issues with the instructions, the following **URL** will allow you to check your Android version.[187]

13.3.2 Through A Wireless Provider

Your wireless provider may have a tool or service that lets you block calls and text messages. The following **URL**, will navigate users to the U.S. wireless communications industry where you can learn about the options from different providers.[188]

13.3.3 Through Call Blocking Apps

Some call-blocking apps also let you block unwanted text messages. Go to the following **URL** for a list of call-blocking apps for[189]:

13.3.3.1 Android [190]

13.3.3.2 BlackBerry [191]

13.3.3.3 Apple [192]

13.3.3.4 Windows [193]

13.4 How To Report Spam Text Messages

If you get an unwanted text message, there are three ways to report it:

13.4.1 Report It On The Messaging App You Use

Look for the choice to report junk or spam.

13.4.1.1 Android

Please navigate to the following **URL** [194]

13.4.1.2 iPhone

Please navigate to the following **URL** [195]

13.4.2 Forward The Message To 7726 (SPAM)

You can copy the message and send it to 7726 (SPAM).

13.4.3 Federal Trade Commission Reporting

You can report spam text messages to the following **URL**.

13.5 Prevent SIM Hijacking

SIM-swapping occurs when a threat actor poses as you to a service provider, using social engineering techniques and information gathered about you to fool employees into transferring ownership of your mobile number.[196]

Once the SIM is swapped, the victim's calls, texts, and other data are diverted to the criminal's device. This access allows criminals to send 'Forgot Password' or 'Account Recovery' requests to the victim's email and other online accounts associated with the victim's mobile telephone number.[197]

Using SMS-based two-factor authentication, mobile application providers send a link or one-time passcode via text to the victim's number, now owned by the criminal, to access accounts. The criminal uses the codes to login and reset passwords, gaining control of online accounts associated with the victim's phone profile.[198]

13.5.1 Safeguard Personal Information

Threat actors start the hijacking process by finding a target and collecting their personal information. They get hold of data like email addresses, mailing addresses, government-issued ID numbers, date of

birth and more by trawling social media, setting up phishing attacks, or buying it from other online fraudsters.[199]

To protect against SIM card swaps, make it hard for hackers to find information about you. Hackers will use data they find about you online, such as names of friends and family or your address. This information will make it easier to convince a customer support agent that they are you.[200]

13.5.2 Set a SIM Card Lock

To protect against SIM attacks, you should also set up some protections on your SIM card. The most important security measure you can implement is to add a PIN code. This way, if anyone wants to change your SIM card, they need the PIN code.

Before you set up a SIM card lock, you should ensure you know the PIN given to you by your network provider.

13.5.2.1 SIM Card Lock on iPhone

- On an iPhone, go to **Settings > Cellular > SIM PIN**. On an iPad, go to **Settings > Mobile Data > SIM PIN**.[201]
- Then enter your **existing PIN** to confirm, and the SIM lock will be activated.

13.5.2.2 SIM Card Lock on Android

- To set it up, on an Android device, go to **Settings > Lock screen and security > Other security settings > Set up SIM card lock.**[202]
- Then, you can enable the slider for **Lock SIM card**.

13.6 Enabling Two-Factor Authentication

To further protect your account beyond your username and password, setting up two-factor authentication will require an added authentication factor like an SMS text message sent to your phone, a code delivered to your email, or a code generated via an authenticator app.[203] If two-factor authentication is unavailable, it is recommended a user setup Security Questions and a PIN for their account.[204]

13.7 Creating Strong Passwords

- For passwords, it is recommended a user employ 14 characters or longer, using upper and lower case, and a mixture of numbers, letters, and special characters.
- Do not share account information, PIN, or passwords.
- A user can also use a password safe. These apps can generate strong passwords for you and then save them to help you fill them in later.

13.8 Setting A PIN At The Account Level

- Adding a PIN or passcode to your account, adds an extra layer of security. To make changes to your account, this PIN is needed.
- Some carriers set the PIN as the last four digits of the primary account holder's SSN, so be sure to change this code to something unique.

- Consider updating the PIN periodically.

13.9 Major Carrier Additional Security Features

The 4 major carriers implement slightly different safeguards for protecting customer accounts.

- **AT&T** has a guide on **how to set up extra security** on your account.[205]
- **T-Mobile** allows you to **set up a customer passcode**.[206]
- **Verizon** explains **how you can add a PIN** to your account.[207]
- **Sprint** also lets you **add an account PIN** for greater security.[208]

14 Personal Credit

14.1 Credit Freeze Overview

Anyone can freeze their credit report, even if their identity has not been stolen. A credit freeze restricts access to your credit report, which means you, or threat actors, will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. When the freeze is in place, you will still be able to do things like apply for a job, rent an apartment, or buy insurance without lifting or removing it. A credit freeze lasts until you remove it.[209]

14.2 Enabling A Credit Freeze

To place a credit freeze, you must contact each of the three credit bureaus. You can request a credit free online or by mail.

14.2.1 Equifax Credit Freeze

To enable a credit freeze for Equifax, you can click on the following **URL**.[210]

14.2.2 Experian Credit Freeze

To enable a credit freeze for Experian, you can click on the following **URL**.[211]

14.2.3 TransUnion Credit Freeze

To enable a credit freeze for TransUnion, you can click on the following **URL**.[212]

14.3 Fraud Alert Overview

Fraud alerts are available in different situations and have different benefits. Anyone who suspects fraud can place a fraud alert on their credit report. A fraud alert will make it harder for someone to open a new credit account in your name. A business must verify your identity before it issues new credit in your name. When you place a fraud alert on your credit report, you can get a free copy of your credit report from each of the three credit bureaus. A fraud alert lasts one year. After a year, you can renew it.[213]

14.3.1 Equifax Fraud Alert

To enable a fraud alert for Equifax, you can click on the following **URL**.[214]

14.3.2 Experian Fraud Alert

To enable a fraud alert for Experian, you can click on the following **URL**.[215]

14.3.3 TransUnion Fraud Alert

To enable a fraud alert for TransUnion, you can click on the following **URL**.[216]

14.4 Extended Fraud Alert Overview

An extended fraud alert is only available to people who have had their identity stolen and completed an FTC identity theft report at the following **URL** or filed a police report. Like a fraud alert, an extended fraud alert will make it harder for someone to open a new credit account in your name.[217]

14.4.1 How To Place An Extended Fraud Alert

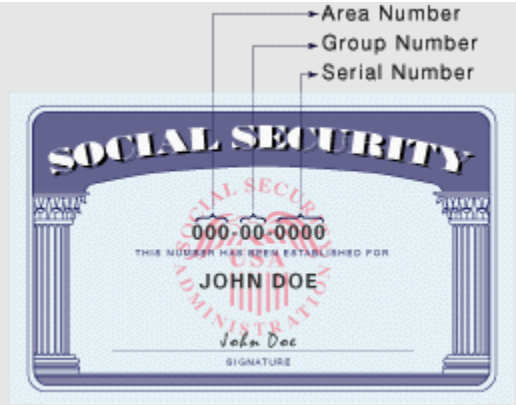
When you place an extended fraud alert on your credit report, you can get a free copy of your credit report from each of the three credit bureaus twice within one year from when you place the alert, which means you could review your credit report six times in a year.[218]

In addition, the credit bureaus will take a user off their marketing lists for **unsolicited credit and insurance offers** for five years, unless you ask them not to.[219] An extended fraud alert lasts seven years and is free. Contact any one of the **three credit bureaus**, Equifax, Experian, and TransUnion. You do not have to contact all three. The credit bureau you contact must tell the other two to place an extended fraud alert on your credit report.[220]

15 SOCIAL SECURITY NUMBER

The following information from the Social Security Administration (SSA) explains how the nine-digit SSAN (aka SSN) is composed of three parts. More available at the following **URL**.[221]

- The first set of three digits is called the ***Area Number***.
- The second set of two digits is called the ***Group Number.***
- The final set of four digits is the ***Serial Number*.**



15.1 AREA NUMBER

The Area Number is assigned by the geographical region. Prior to 1972, cards were issued in local Social Security offices around the country and the Area Number stood for the State in which the card was issued. This did not necessarily have to be the State where the applicant lived, since a person could apply for their card in any Social Security office.

- Since 1972, when SSA began assigning SSNs and issuing cards centrally from Baltimore, the area number assigned has been based on the ZIP code in the mailing address provided on the application for the original Social Security card.
- The applicant's mailing address does not have to be the same as their place of residence. Thus, the Area Number does not necessarily stand for the State of residence of the applicant, prior either to 1972 or since.
- Numbers were assigned beginning in the northeast and moving westward.
- Therefore, people on the east coast have the lowest numbers and those on the west coast have the highest numbers.
- In 2007, the SSA gave public notice that it intended to abandon its earlier method for choosing Social Security numbers and instead to go to a random process for assignment.[222] The SSA followed through with that change in June 2011.

15.2 GROUP NUMBER

Within each area, the group number (middle two (2) digits) range from 01 to 99 but are not assigned in consecutive order.

- For administrative reasons, group numbers issued first consist of the ODD numbers from 01 through 09 and then EVEN numbers from 10 through 98, within each area number distributed to a State.
- After all numbers in group 98 of a particular area have been issued, the EVEN Groups 02 through 08 are used, followed by ODD Groups 11 through 99.

15.3 Serial Number

Within each group, the serial numbers (last four (4) digits) run consecutively from 0001 through 9999. When the government introduced the Social Security program with its numbers in 1936, it was never meant to be so widely used to find and track individuals.

- Today, this number is used for everything from its original purpose – to track your lifetime earnings and calculate your Social Security benefits – to opening a checking account or fill out a new-patient form at the doctor's office.
- In the United States, many businesses will ask for your Social Security number simply because it is a convenient way for them to find customers.
- Unfortunately, threat actors can use your Social Security number to commit identity theft, so you should always guard your Social Security number carefully and only give it out when necessary.

15.4 Protecting Your SSN

Now that you understand what makes up an SSN, here are some simple ways you protect your SSN:

15.4.1 Alternative Form Of Identification

If a business or organization asks for your Social Security number, offer your driver's license number instead.

- Other alternative forms of ID include a passport, proof of current and earlier address (bills) or even a student ID from a college or university.

15.4.2 Ask Why And How

If the business insists, ask questions. You have a right to know why it is necessary to supply your SSN and how it will be handled. Here are some questions:

- Why is having my SSN necessary?
- With whom will you share my SSN with if I provide it?
- How will my SSN be stored? Will it be encrypted?
- Do you have a privacy policy, and may I see it?
- Will you cover my liability or losses if my SSN is stolen or compromised?
    - Unfortunately, if you are asked to supply your SSN by a business or institution that does not need it and you say no, it can refuse to supply services to you or put conditions on the service—such as a deposit or added fees. However, the question to always ask is "do I want to do business with a business that does not care about my privacy concerns?"

15.4.3 Leave Your Card At Home

Do not carry your card around with you in your wallet or purse.

- Do not enter it into your phone, laptop, or other device. It is unlikely you will need your card and when you do need it, it does not come as a surprise.

15.4.4 Shred Mail And Documents

Discarded mail and documents are easy places for identity thieves to search. Do not just throw out papers that hold personal details such as your SSN.

- Get a shredder at a discount or office supply store and use it on a regular basis.
- Do not leave mail in an outside mailbox for prolonged periods. Stealing mail is another way a thief can make off with your identity.

15.4.5 Do Not Use Your SSN As A Password

Do not use the whole number—or part of it—as a password for anything! The password file can be stolen and decrypted, or someone can just watch you type it in from over your shoulder.

- Also, if you need to require it for legitimate purposes in a public place, be careful who may be able to eavesdrop on your conversation.

15.4.6 Do Not Send Your SSN Electronically

Never type your SSN into an email or instant message and send it. Most email messages can be intercepted and read in transmission.

- Also, do not leave a voice mail that includes your SSN. If you need to contact someone and give them your number, it is always best to do so in person.
- If you need to do so on the phone, ensure you are speaking to the right person, so you are not swindled.

15.4.7 Do Not Give Your SSN Out

You should never supply your SSN to someone you do not know who calls you on the phone and requests it. This same warning applies to unsolicited emails and any forms you fill out on the internet.

- In general, do not give your SSN to anyone unless you are certain they have a reason and a right to have it.

15.4.8 Monitor Bank And Credit Card Accounts

Keep close tabs on your bank and credit card balances.

- This is one way to make sure your SSN and identity have not been compromised.
- Many banks let you sign up for account alerts. They will send you text alerts or call you if transactions exceed a certain amount or if someone tries to use your SSN to access your account.
- You can also check your credit score on a regular basis at AnnualCreditReport.com. You can do this once a year free.[223]
- If the Social Security Administration is still sending you an annual statement detailing your earnings, and it looks abnormal, someone might be using your SSN for employment purposes. You can register to get statements at the Social Security Administration's **URL**.[224]

15.4.9 Use An Identity Protection Service

You can register with (and pay for) an identity protection service such as **LifeLock**, **IdentityForce**, or **Identity Guard**.

- Such services supply identity insurance—for a fee, that typically starts around $10 per month.
- Banks and credit unions also have packages they sell to customers, as do major credit rating agencies such as Experian and TransUnion.

15.4.10 Protect Your Child's SSN

- While you are protecting your own Social Security number, make sure you are equally watchful about your children's numbers.

15.4.11 Block Access To Your SSN

If you know your Social Security information has been compromised, you can request to Block Electronic Access. This is done by calling their national 800 number (Toll Free 1-800-772-1213 or at their TTY number 1-800-325-0778).[225]

- Once requested, any automated telephone and electronic access to your Social Security record is blocked. No one, including you, will be able to see or change your personal information on the internet or through our automated telephone service.
- If you have requested that we block access to your record and change your mind in the future, you can contact us and ask to have the block removed. You will need to prove your identity when you call.

15.4.12 E-Verify

E-Verify, authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), is a web-based system through which employers electronically confirm the employment eligibility of their employees.

- E-Verify is administered by SSA and U.S. Citizenship and Immigration Services (USCIS). USCIS facilitates compliance with U.S. immigration law by supplying E-Verify program support, user support, training, and outreach, and developing innovative technological solutions in employment eligibility verification.[226]

15.4.12.1 E-Verify Self Lock

Self-Lock is the unique feature that lets you protect your identity in E-Verify and Self Check by placing a "lock" on your Social Security number (SSN).

- This helps prevent anyone else from using your SSN to try to get a job with an E-Verify employer.
- If an employer enters your locked SSN in E-Verify to confirm employment authorization, it will result in an E-Verify mismatch, called a **Tentative Nonconfirmation** (TNC).[227]

15.4.12.2 Using E-Verify Self Lock

To access Self Lock, you must be logged in to your **myE-Verify account.**[228] To lock your SSN, you must enter your SSN and date of birth. myE-Verify does not store your SSN when you create your account, so you must supply your SSN to "lock" it. [229]

- In addition, you must select and answer three challenge questions. Select questions you can easily answer, because you will need to answer them again to verify your identity if you receive an ***E-Verify Tentative Nonconfirmation*** due to Self-Lock.

16 ONLINE REAL ESTATE LISTINGS

You should consider removing pictures of your home from real estate services' online listings. These often display both exterior and interior images of your residence.

- Further privacy can be achieved by suppressing curbside images of your home from showing in Google Street View and Bing Curbside. More advice can be at this **URL**.[230]

16.1 REAL ESTATE ONLINE SERVICE PRIVACY LINKS

Service	Privacy Settings
Zillow	https://zillow.zendesk.com/hc/en-us/articles/218578357-Owner-Dashboard https://zillow.zendesk.com/hc/en-us/requests/new
Trulia	https://support.trulia.com/hc/en-us/requests/new
Realtor	Sign up, control of listing
Redfin	https://support.redfin.com/hc/en-us/articles/360013247432-Removing-Photos-on-a-Sold-Home
Movoto	Contact customercare@movoto.com
Homesnap	Contact support@homesnap.com

16.2 REMOVING CURBSIDE PICTURES OF YOUR HOME

Service	Privacy Settings
Google Street View	https://www.wikihow.com/Opt-Out-of-Google-Street-View https://support.google.com/websearch/answer/4628134?hl=en
Bing Streetside	https://www.bing.com/maps/privacyreport/streetsideprivacyreport?bubbleid=198628406

17 WI-FI, BLUETOOTH, NEAR FIELD COMMUNICATION AND MAC ADDRESS

Threat actors can compromise devices over public Wi-Fi, Bluetooth, and Near-Field Communications (NFC), a short-range wireless technology.[231] This puts personal and organizational data, credentials, and devices at risk.

- Devices include laptops, tablets, mobile, wearable, and others that can connect to public wireless technologies.
- The guidance throughout helps users understand the risks in using public wireless technologies and enables them to make calculated decisions about the level of risk they accept.
- At a minimum, it is recommended users disable Wi-Fi, Bluetooth, and NFC when not in use.[232]

17.1 WI-FI OVERVIEW

There are two kinds of Wi-Fi networks: secured and unsecured.[233] Most Wi-Fi networks that are created for home and business uses are password-protected and encrypted.[234]

- However, most public Wi-Fi hotspots are set up strictly for convenience – not security.[235]
- An unsecured Wi-Fi network can be connected to within range and without any type of security feature like a password or login.[236]
- In contrast, a secured network requires a user to agree to legal terms, register an account, or type in a password before connecting to the network.[237]

17.1.1 Public Wi-Fi Recommendations

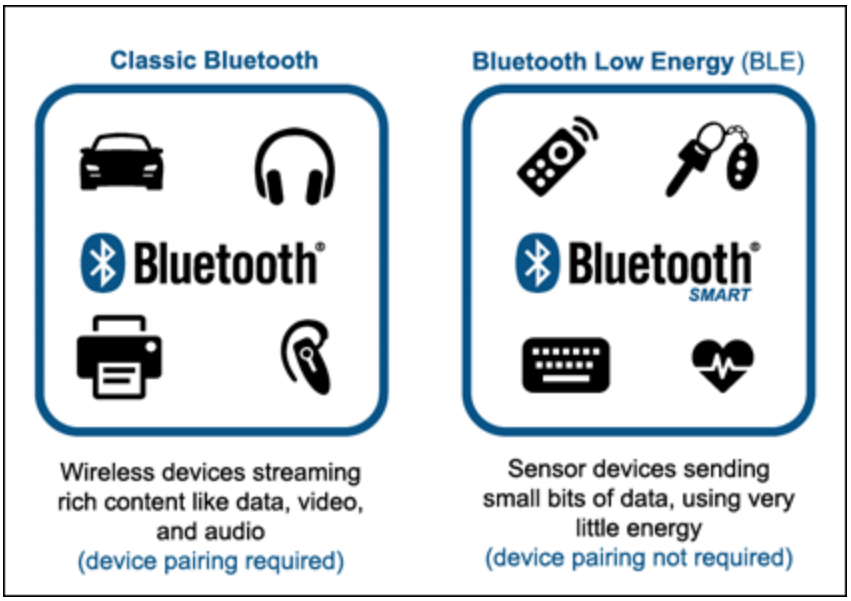
If you need to connect to a public wireless hotspot, it is recommended you use a virtual private network (VPN) to encrypt your web traffic. Do not connect to networks if you are not familiar with them or cannot verify their authenticity.[238]

It is recommended that you DO NOT:

- Allow your Wi-Fi to **auto-connect** to networks.[239]
- Log into any account via an app that has sensitive information. Go to the website instead and verify it uses **HTTPS before** logging in.
- Leave your **Wi-Fi** or **Bluetooth** on if you are not using them.
- Access websites that hold your sensitive information, such as such as financial or healthcare accounts.[240]
- Log onto a network that is **not** password protected.

It is recommended that you DO

- Disable **file sharing**
- Only visit sites using **HTTPS**.
- **Log out** of accounts when done using them.
- Use a **VPN**, like Norton Secure VPN, to make sure your public Wi-Fi connections are made private.



17.1.2 Home Wireless Network Security

Home wireless networks enable computers and mobile devices to share one broadband connection to the internet without having to use up minutes on cellular data plans.[241] But like all other wireless network technologies, home wireless networks present vulnerabilities that could be exploited by hackers.[242] To help protect your home wireless network from unwanted users, consider the following steps:

- Change the network's default network name, also known as its service, set identifier or "SSID." When a computer with a wireless connection search for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. Manufacturers usually give all their wireless routers a default SSID, which is often the company's name. For added security, choose a unique and hard to guess name as your SSID.[243]
- Change the network's default password. Most wireless routers come with preset passwords for administering a device's settings (this is different from the password used to access the wireless network itself). Unauthorized users may be familiar with the default passwords, so it is important to change the router device's password as soon as it is installed. Longer passwords made up of a combination of letters, numbers and symbols are more secure.[244]
- Consider using the Media Access Control, or "MAC," address filter in your wireless router. Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept connections only from devices with MAC addresses that the router will recognize. To create another obstacle to unauthorized access, consider activating your wireless router's MAC address filter to include your devices only.[245]
- Turn off your wireless router when it will not be in use for any extended period.[246]
- Use anti-virus and anti-spyware software on your computer and use similar apps on your devices that access your wireless network.

17.1.2.1 Implement WPA2 On The Wireless Network

- To keep your wireless communication confidential, ensure your personal or ISP-provided WAP is using Wi-Fi Protected Access 2 (WPA2). When configuring WPA2, use a strong passphrase of 20 characters or more.[247]
- Most computers and mobile devices should now support WPA2. When finding a suitable replacement, ensure the device is WPA2-Personal certified.[248]
- Change the default SSID to something unique. Do not hide the SSID as this adds no other security to the wireless network and may cause compatibility issues.[249]

17.1.3 Wi-Fi Tracking Opt Out

Wi-Fi location tracking is a geolocation system that uses the entire Wi-Fi infrastructure (phones, tablets, laptops, and routers) as Wi-Fi access points to find a device's location. Even when a user is not connected to a router, their device is still sending and receiving data to discover nearby routers, so the devices are still in constant communication as long as the user has Wi-Fi enabled.[250]

The simplest way to prevent Wi-Fi location tracking is for a user to turn off their Wi-Fi when not connected to a trusted Wi-Fi connection. The following websites will also allow users to opt out of location tracking services.

Service	Website
Here	https://legal.here.com/us-en/here-wi-fi
Future of Privacy Forum: Smart Place Privacy	https://optout.smart-places.org/
SkyHook	https://www.skyhook.com/opt-out-of-skyhook-products
Microsoft	https://account.microsoft.com/privacy/location-services-opt-out
Basking	https://basking.io/opt-out/

17.1.4 Hiding a Wi-Fi Network

Wi-Fi networks are found by their network name, known as a *service, set identifier (SSID)*. Some Wi-Fi networks are configured to hide their SSID, which results in the wireless access point not broadcasting the network's name. These are known as *hidden networks*. iPhone 6s and later devices automatically detect when a network is hidden. If a network is hidden, the iOS or iPadOS device sends a probe with the SSID included in the request—not otherwise. This helps prevent the device from broadcasting the name of previously hidden networks a user was connected to, thereby further ensuring privacy.[251]

17.2 Bluetooth Overview

Bluetooth is the technology that enables exchange of data between devices within a short amount of distance.

- What separates Bluetooth radio waves from the broadcast sent out by a radio station is the fact that Bluetooth waves do not travel extremely far and are constantly switching frequencies.
- Most Bluetooth devices have a maximum connectivity range of about 30 feet, and that distance is reduced when obstacles are present.[252]

- Bluetooth Low Energy (BLE)—also known as Bluetooth Smart—is the latest version of Bluetooth technology that offers significantly less power consumption and costs compared to Classic Bluetooth while still supporting a similar communication range.[253]
- Bluetooth and Wi-Fi are often complementary, working at the same time and offering much the same connectivity, you may not always know which hardware is pairing with which devices.
- Just know that if in range, devices previously paired via Bluetooth will try to automatically connect.[254]

17.2.1 Bluetooth As An Attack Vector

There have been many noteworthy Bluetooth vulnerability discoveries in recent years and the sophistication of the attacks will only evolve.[255]

- Disturbingly, hackers no longer need to be nearby the devices to carry out their exploits.[256] Bluetooth was designed for short-range communications, but because they have radios, cyber thieves can exploit a system remotely and then use that system's Bluetooth interface to launch an attack.
- In this role, it is possible for an attacker to not only run these attacks remotely while in proximity, but also conduct them from much further away using low-cost equipment.

17.2.2 Notable Bluetooth Vulnerabilities

As a result of an attackers' ability to implement remote attacks via radio, the increasing threat from Bluetooth devices to network security is a top concern for security teams. Here are the top eight recent Bluetooth vulnerability discoveries[257] that organizations have had to address:

17.2.2.1 BIAS (Bluetooth Impersonation AttackS)

Earlier this year, a new Bluetooth flaw dubbed BIAS was discovered with the potential to expose billions of devices to hackers. BIAS allows cyber-criminals to create an authenticated Bluetooth connection between two paired devices without needing a key.[258]

- The attacker can take over communication between the two devices by impersonating either end such as a mouse or a keyboard, giving the intruder inside access to the targeted device.[259]
- Once inside, the masquerading attacker can then implement malicious exploits such as stealing or corrupting data.[260]

17.2.2.2 BleedingBit

The attacker can use Bluetooth Low Energy (BLE) implementation vulnerabilities for remote code execution[261] and total machine take over to infiltrate networks.[262]

17.2.2.3 BlueBorne

An attacker can actuate carefully constructed packets to cause buffer overflows[263] which can be exploited for code execution.[264]

- The attacker can then take over a machine running Bluetooth Classic and use it as a potential entry point for malicious activity.[265]

17.2.2.4 Bluetooth Denial of Service (DoS) Via Inquiry Flood

This DoS attack targets BLE devices, running down their batteries and preventing them from answering other requests from legitimate devices.[266]

- This is particularly concerning for medical devices being used in life-saving situations.[267]

17.2.2.5 Fixed Coordinate Invalid Curve Attack

Hackers can crack the encryption key for both Bluetooth and BLE because of subtle flaws in the Elliptic Curve Diffie- Hellman key exchange process.[268]

- Attackers can imitate devices, inject commands, and penetrate for added security flaws.[269]

17.2.2.6 KNOB (Key Negotiation of Bluetooth)

An attacker can crack encryption on a Bluetooth conversation and then snoop to see all encrypted traffic as if it was plaintext.[270]

- The attacker can erase or inject packets, and ransom or publish the captured details.[271]

17.2.2.7 Malicious Applications Leveraging Radio Frequency Interfaces

Leveraging a downloaded app, a cybercriminal can access an iPhone's camera and microphone without permission.

- The attacker can then record and exfiltrate audio and video, and then ransom or publish the compromised information.[272]

17.2.2.8 Sweyntooth

An attacker within radio range can trigger deadlocks, crashes, and buffer overflows or completely detour security by sending faulty packets over the air.[273]

- If successful, this could result in the crash of devices such as medical equipment, potentially causing harm to patients, or other IoT connected devices in offices or homes.[274]

17.2.3 Bluetooth Beacons

If you own a business or are involved in marketing, you have some level of understanding about how beacon technology works[275] and you may have even received a Google beacon as part of Project Beacon[276], a program Google launched[277] to send free beacons to businesses with the aim of enabling proximity-based triggers and actions in both the digital and physical world. This Digital Exhaust is based on location-tracking data, gleaned from mobile phone users who have their Bluetooth enabled by default or by accident, as many people do.[278]

- With the emergence of COVID-19 in 2020, the issue of just how valuable and detailed our collective Digital Exhaust is has been proven by both Google[279] and Facebook[280] who began sharing location-tracking information with various authorities around the world to help them plan their COVID-19 containment strategies.
- The data supplied is "anonymized" and "aggregated", so there are no personally identifying markers. But the data does track people's movements - for example, Google's Mobility Reports[281], which it is made available for 131 countries and regions, show foot traffic trends at various locations over time.

17.2.4 Securing Bluetooth

As a wireless data transfer standard, Bluetooth has some associated cybersecurity risks. You do not want unauthorized parties to access the data you are transferring via Bluetooth, nor do you want them to have access to your Bluetooth-enabled devices.

- It helps to know what the security risks with Bluetooth are so you can enjoy all the convenience of the widespread wireless technology while mitigating its risks.

17.2.4.1 Physically Secure Your Device

You may want to set up a "find my device" service on your phone through a trustworthy entity like Apple or Google so you have a way of using their technologies to find and remotely lock your device if you lose it.

17.2.4.2 Avoid Using Bluetooth to Communicate Sensitive Information

If you choose to use Bluetooth to transfer sensitive information from your device to another device, consider encrypting your files first.

17.2.4.3 Turning Off Bluetooth Discoverable Mode

- Ensure you turn off Bluetooth discoverable modes after pairing a new peripheral with your device.
- Once paired, you do not need to have discoverable mode on because your device will already know the peripheral's unique identifying code.
- This will also secure your device from any unwanted pairing attempts.

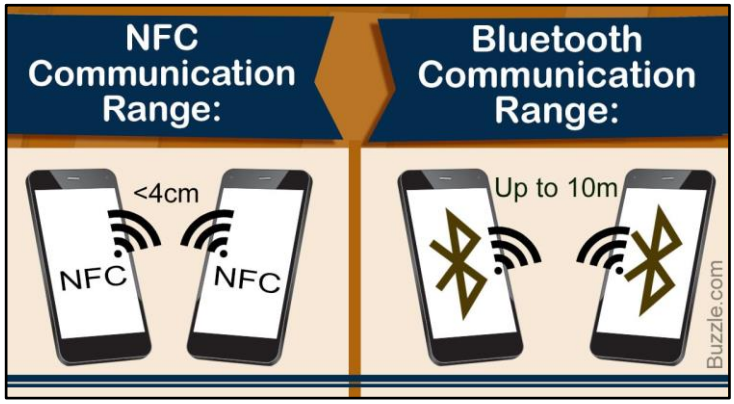
17.2.4.4 Bluetooth Opt Out

To opt out your Bluetooth address please use the following **URL.**

17.3 Near Field Communication Overview

Bluetooth and Wi-Fi while like near field communication on the surface, do have distinct differences.

- All three allow wireless communication and data exchange between digital devices like smartphones.
- Yet near field communication uses electromagnetic radio fields while technologies such as Bluetooth and Wi-Fi focus on radio transmissions instead.[282]



Near field communication, or NFC for short, is an offshoot of radio-frequency identification (RFID) with the exception that NFC is designed for use by devices within close proximity to each other.

- Devices using NFC may be active or passive. A passive device, such as an NFC tag, holds information that other devices can read but does not read any information itself. Think of a

passive device as a sign on a wall. Others can read the information, but the sign itself does nothing except send the info to authorized devices.[283]

- Active devices can read information and send it. An active NFC device, like a smartphone, would not only be able to collect information from NFC tags, but it would also be able to exchange information with other compatible phones or devices and could even alter the information on the NFC tag if authorized to make such changes.

To ensure security, NFC often sets up a secure channel and uses encryption when sending sensitive information such as credit card numbers.

- Users can further protect their personal data by keeping anti-virus software on their smartphones and adding a password to the phone so a thief cannot use it if the smartphone is lost or stolen.[284]
- Unaccustomed users of near field communication, especially for payment purposes such as storing credit card information, may be concerned about the security and safety of their confidential information.

17.3.1 NFC Vulnerabilities

Security attacks include eavesdropping, data corruption or modification, interception attacks, and physical thefts. Below we cover the risks and how NFC technology works to prevent such vulnerabilities:

17.3.1.1 Eavesdropping

Eavesdropping is when a criminal "listens in" on an NFC transaction. The criminal does not need to pick up every single signal to gather confidential information. Two methods can prevent eavesdropping.

- First there is the range of NFC itself.
- Since the devices must be close to send signals, the criminal has a limited range to work in for intercepting signals. Then there are secure channels.
- When a secure channel is set up, the information is encrypted and only an authorized device can decode it.
- NFC users should ensure the companies they do business with use secure channels.

17.3.1.2 Data Corruption And Manipulation

Data corruption and manipulation occur when a criminal manipulates the data being sent to a reader or interferes with the data being sent so it is corrupted and useless when it arrives.

- To prevent this, secure channels should be used for communication.
- Some NFC devices "listen" for data corruption attacks and prevent them before they have a chance to get up and running.

17.3.1.3 Interception Attacks

Like data manipulation, interception attacks take this type of digital crime one step further. A person acts as a middleman between two NFC devices and receives and alters the information as it passes between them. This type of attack is difficult and less common.

- To prevent it, devices should be in an active-passive pairing.

- This means one device receives info and the other sends it instead of both devices receiving and passing information.

17.3.1.4 Theft

No amount of encryption can protect a consumer from a stolen phone. If a smartphone is stolen, the thief could theoretically wave the phone over a card reader at a store to make a purchase.

- To avoid this, smartphone owners should be diligent about keeping tight security on their phones.
- By installing a password or other type of lock that appears when the smartphone screen is turned on, a thief may not be able to figure out the password and thus cannot access sensitive information on the phone.
- Through data encryption and secure channels, NFC technology can help consumers make purchases quickly while keeping their information safe at the safe time.

17.4 MAC Address Overview

A Media Access Control address (MAC address) is a hardware identifier that uniquely shows each device on a network. Primarily, the manufacturer assigns it. They are often found on a device's network interface controller (NIC) card. A MAC address can also be referred to as a burned-in address, Ethernet hardware address, hardware address, or physical address. A MAC address is a 48-bit hexadecimal address. It is usually six sets of two digits or characters, separated by colons. An example MAC address would be 00:00:5e:00:53:af.

Many network cards and other hardware manufacturers use a unique sequence at the beginning of their products' MAC addresses. This is called an organizationally unique identifier (OUI). The OUI is usually the first three bytes of digits or characters. The **IEEE (Institute of Electrical and Electronics Engineers) administers manufacturers' OUIs**.

17.4.1 How To Find A MAC Address

17.4.1.1 iOS

- Go to **Settings > General > About**.
- The **Wi-Fi Mac Address** is displayed in the field labeled "Wi-Fi Address".
- **Long press** this field and then select "copy".
- The Mac Address can now be pasted anywhere.

17.4.1.2 Mac OS

- Go to **System Preferences > Network**
- Select **Wi-Fi** on the left side **>** click on the "**Advanced**…" button on the right.
- The Mac address is visible in the "**Hardware**" tab.

17.4.1.3 Android

- Go to **Menu > Settings > Wireless & Networks**.
- Check the box marked **Wi-Fi** to ensure that wireless is turned on.
- Go to **Back > About Phone** or **About Tablet > Hardware Information**.

- The **Wi-Fi Mac Address** is displayed there.
- Copy the **Mac Address**.

17.4.1.4 Windows

- Make sure your **Wi-Fi** is enabled.
- Go to **Start > Settings > Connections > Wireless LAN > Advanced**.
- The address is displayed in the "**MAC**" field.

17.4.2 MAC Address Randomization

MAC randomization helps ensure the privacy of your mobile device by concealing the original MAC address, making it significantly harder to track a device based on its MAC address especially when connecting to public hotspots.[285]

MAC randomization is a process that hides the exact identity of a mobile device. It works by concealing what is called the media access control (MAC) address of that device and creating an artificial one in its place, which is then transmitted to any surrounding Wi-Fi access points.[286]

17.4.3 Apple Private MAC Address

Starting with iOS 14, iPadOS 14, and watchOS 7, Apple allows a user's device to use a different MAC address for each Wi-Fi network. This unique MAC address is your device's private Wi-Fi address, which it uses for that network only.[287]

17.4.3.1 iPhone, iPad, or iPod touch

- Open the **Settings** app, then tap **Wi-Fi**.
- Tap the **information button** ⓘ next to a network.
- Tap to turn **Private Address** on or off.
- If your device joined the network without using a private address, a privacy warning explains why.

17.4.3.2 Apple Watch

- Open the **Settings** app, then tap **Wi-Fi**.
- Tap the name of the **network** you joined. If you have not joined the network yet, swipe left on its name and tap **more** ••• .
- Tap to turn **Private Address** on or off.

17.4.4 Android Private MAC Address

In Android 10, MAC randomization was enabled by default for client mode, SoftAp, and Wi-Fi Direct. Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations.[288] [289]

17.4.4.1 Android 10 And Later Versions

- Go to the **Settings** app on your Android device.
- Tap on **Network & Internet or Connections** > **Wi-Fi**.
- Tap the **gear** icon next to the **Wi-Fi** name of your choice.
- Tap on **MAC address type**.
- Select **Use phone MAC**.
- Turn **OFF** your device's Wi-Fi and then **ON** again.

17.4.4.2 Samsung Galaxy Devices

- Go to the **Settings** app on your Android device.
- Tap on **Connections** > **Wi-Fi**.
- Tap the **gear** icon next to the **Wi-Fi** name of your choice.
- Tap on **MAC address type**.
- Select **Use phone MAC**.
- Turn **OFF** your device's Wi-Fi and then **ON** again.

17.4.5 MAC Address Opt Out

Many cell phones have Wi-Fi or Bluetooth capabilities built into them so you can do things like access the Internet or use a hands-free device. Your cell phone broadcasts a Wi-Fi MAC Address or Bluetooth MAC address – a 12-digit string of letters and numbers assigned to your phone by its manufacturer that allows it to be detected by nearby Wi-Fi or Bluetooth sensors. Venues use MLA technology – such as beacons or sensors – to detect when nearby cell phones broadcast their MAC addresses.[290] To opt out your MAC address please use the following **URL**.

18 Debit And Credit Card Tracking

Although it is illegal for financial institutions to sell your information, sharing your information is often important for their business operations and your information to be shared internally and with affiliates and non-affiliates.[291]

- Affiliates are companies related by control or ownership, and non-affiliates are outside companies. The companies can be financial or non-financial in nature. Companies share your information with both parties to market to you.[292]
- Some companies often claim a user's privacy would not be violated as all personal data has been de-identified and pseudonymized, (i.e., your personal information) like name and credit card number have been replaced by pseudonyms.
- If you would like to know more about privacy choices for your personal financial information, read the article by the Federal Trade Commission **URL** and review the list of specific banks and credit card privacy opt-out links at **URL**.

18.1 Debit and Credit Card Financial Opt Out

Service	Privacy Settings
MasterCard	https://www.mastercard.com/global/en/vision/corp-responsibility/commitment-to-privacy/privacy/data-analytics-opt-out.html
Visa	https://privacy.visa.com/dsarwebform/e47650b1-4525-441b-96dc-35a5fb22617e/f934d161-867b-4ee0-8070-a844292a2e05.html
American Express	https://help.line.me/line/?contentId=20002865
Discover	https://www.linkedin.com/help/linkedin/answer/92055/understanding-your-privacy-settings?lang=en

19 SOCIAL MEDIA PLATFORMS

The role of social media in our lives continues to grow each year and so too does the amount of personal information which can be found through our online personas.[293] [294]

- While who and what we share through social media is a personal choice[295], it is recommended that you be intentional about who you share your data with[296], to include which sites and platforms that you trust and consider worth the risk.
- The role of the section below is to inform you of several privacy settings to aid you in securing your social network accounts so that you only share information with people you choose and not those you do not.
- Online social media services are teeming with private and public personal information.[297] [298]
- Control yours via the below links to privacy settings.
- Further, ensure your account usernames and/or account unique IDs ***do not*** correlate with your personal data, and do not respond to messages or accept connection requests from parties you do not know or cannot confirm to be legitimate.
- Accessing social media applications from open Internet hotspots provided at hotels, cafés, and airports may leave devices susceptible for adversaries to spy on activities physically and virtually.[299]
- Adversaries can also access devices and information if Bluetooth® and Wi-Fi® are enabled.[300]

19.1 Social Media Privacy Settings Links

Service	Privacy Settings
Facebook	https://www.facebook.com/about/basics
Instagram	https://help.instagram.com/196883487377501
Line	https://help.line.me/line/?contentId=20002865
LinkedIn	https://www.linkedin.com/help/linkedin/answer/92055/understanding-your-privacy-settings?lang=en
Pinterest	https://help.pinterest.com/en/article/edit-account-privacy
Skype	https://support.skype.com/en/faq/FA140/how-do-i-manage-my-privacy-settings-in-skype-for-windows-desktop
SnapChat	https://support.snapchat.com/en-US/a/privacy-settings2
Tumblr	https://tumblr.zendesk.com/hc/en-us/articles/115011611747-Privacy-options
Twitter	https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public
Viber	https://support.viber.com/customer/en/portal/topics/592905-security-and-privacy/articles
WeChat	https://help.wechat.com/cgi-bin/newreadtemplate?t=help_center/topic_list&plat=2&lang=en&Channel=helpcenter&detail=1003386
WhatsApp	https://faq.whatsapp.com/en/android/23225461/?category=5245250
YouTube	https://support.google.com/youtube/answer/157177?co=GENIE.Platform%3DDesktop&hl=en

19.2 Discord

Discord is organized into chat groups called servers, which can be public or private. Private, invite-only servers are by far the most common type and typically host no more than 10-15 members. Popular public servers, on anything from a celebrity to a hot topic, can attract thousands of members. All conversations are opt-in, so users must join a server to access content and exchange messages with other people on the server. There is no algorithm delivering content to a newsfeed like other social apps. It should be noted that anyone can start a server.

19.2.1 Servers And Channels

Servers are organized into subtopics called channels. Channels are divided into text and voice channels. In text channels, users post messages, upload files, and share images. In voice channels, users communicate through voice or video chat and screen share (called “Go Live” on Discord). Users can send private messages via voice, video, or text to an individual or group of up to nine other people. Messages are not watched by Discord unless there is an issue. Discord does not offer end-to-end encryption.

19.2.2 Student Hubs

Discord also features Student Hubs, a space for students to engage with others at their school by verifying their Discord account with their official student email. Within the hub, they can connect with other verified students, discover servers for study groups or classes, and share their own servers for fellow students to join. Hubs are student-created and not affiliated with or managed by a school.

Discord has general Community Guidelines against hate speech, harassment and other harms like bullying and misinformation. Servers also have rules that users must accept to join.[301]

Volunteer moderators, or "mods," enforce the rules and remove content or ban users that break the rules. Verified moderators have completed Discord's Moderator Academy, which offers courses on managing and improving Discord communities.[302]

19.2.3 Joining Discord

Users must be 13 or older to join. Discord users choose any username and receive a four-digit number. The username and the four-digit number make up a user's Discord tag. As with most online services, teens need to sign up for Discord using their correct birth year. Discord has default settings designed to keep minors safe, such as automatically scanning direct messages for explicit images and videos.

19.2.4 Safety Considerations

In general, Discord will recommend the most restrictive settings for users under 18 but acknowledge that every teen is unique. Whatever settings are selected by a user, revisiting them periodically is recommended.

19.2.5 Two-Factor Authentication

It is recommended that users enable two-factor authentication for added protection.[303]

- Go to **User Settings > My Account > Enable Two Factor Auth**.
- You can use authenticator apps on a mobile device to authorize access to your account.
- Once two factor authentication is enabled, you will have the choice to further increase your account's security with SMS Authentication by adding your phone number to your Discord account.

19.2.6 Filtering Out Explicit Media

- Go to **User Settings > Privacy & Safety > Safe Direct Messaging**.

Discord recommends the most restrictive setting. **"Keep me safe"** as the default for minor accounts, which means Discord will scan all direct messages for sexually explicit and violent images and videos. If explicit media is found, Discord will remove the message. Minor accounts also cannot access channels labeled **"NSFW,"** or **Not Safe for Work**. Users trying to access channels labeled **NSFW**, which may have nudity or other adult content, must confirm they are at least 18 before entering.

19.2.7 Managing Friends

- Go to **User Settings > Privacy & Safety > Who Can Add You as a Friend**.
- Options include **Everyone**, **Friends of Friends**, and **Server Members**.
- Discord recommends teens only accept friend requests from people they know in real life and that they choose the most restrictive choice, **Friends of Friends**.
- All friend requests must be approved by the user no matter the friend setting.

19.2.8 Direct Messages

- Go to **User Settings > Privacy & Safety > Server Privacy Default**.
- Discord recommends the most restrictive settings for minors.
- "**Allow Direct Messages from Server Members"** is on by default, so toggle it to the off position.
- It should be noted that changes to global settings only affect new servers a user joins.
- To make changes to settings in existing servers, go to **Server Settings** on the server's dropdown menu, which is next to the server's name.

- You can adjust settings on a **server-by-server** basis, so you may want to select the most restrictive settings in the general settings menu and then adjust an individual server's settings to be less restrictive (e.g., a server set up for a study group at school).

19.3 Secure Your Discord Account

19.3.1 Choose A Secure Password

- Having a strong password is key to protecting your account.
- Discord recommends you choose a long password with a mix of uppercase letters, lowercase letters, and special characters that is hard to guess and that you do not use for anything else.
- Discord recommends checking out password managers, which make creating and storing secure passwords extremely easy.
- Discord will require your password to be at least 8 characters long.

19.3.2 Privacy & Safety Settings

Discord gives you control over who can contact you and what they can send you. You can access them by going into your **User Setting*s*** and selecting **Privacy & Safety**.

19.3.3 Age-Restricted Content Media Settings

Users can decide whether they want Discord to automatically scan and remove direct messages that have explicit media content.

- **Keep me safe** - With this setting, images and videos in **all** direct messages are scanned by Discord and age-restricted content is blocked.
- **My friends are nice** - With this setting, all direct messages sent by users who are not on your Friends List are scanned and age-restricted content is blocked. *This setting is good for those who trust their friends not to send content that they would not want to see.* This setting is on by default.
- **Do not scan** - With this setting, **none** of the direct messages you receive will be scanned or blocked for age-restricted content.

19.3.4 Direct Messages (DM) Settings

You might only want certain people to contact you. By default, whenever you are in a server with someone else, they can send you a direct message (DM).

- You can toggle "**Allow Direct Messages from Server Members"** to block DMs from users in a server who are not on your friends list.
- If you have joined any servers prior to turning this off, you will need to adjust your DM settings individually for each server that you have joined.
- To change this setting for a specific server, select **Privacy Settings** on the server's dropdown list and toggle **"Allow Direct Messages from Server Members".**

19.3.5 Friend Request Settings

Discord offers different options for friend request settings.

- **Everyone** - Selecting this means that anyone who knows your Discord Tag or is in a mutual server with you can send you a friend request. This is handy if you do not share servers with someone and you want to let them friend you with just your Discord Tag.

- **Friends of Friends** - Selecting this means that for anyone to send you a friend request, they must have at least one mutual friend with you. You can view this in their user profile by clicking the **Mutual Friends** tab next to the **Mutual Servers** tab.
- **Server Members** - Selecting this means users who share a server with you can send you a friend request. Unselecting this means that you can only be added by someone with a mutual friend.
- If you do not want to be open to **ANY** requests, you can deselect all three options. However, you can still send out requests to other people.

19.3.6 Block Other Users When Needed

When you block someone on Discord, they will be removed from your friends list (if they were on it) and will no longer be able to send you DMs. Any message history you have with the user will remain, but any new messages the user posts in a shared server will be hidden from you, though you can see them if you wish.

19.3.6.1 On Desktop

- Right-click the users **@Username** to bring up a menu.
- Select **Block** in the menu.

19.3.6.2 On Mobile

- Tap the users **@Username** to bring up the user's profile.
- Tap the **three dots** in the upper right corner to bring up a menu.
- Select **Block** in the menu.
- To report a user who is posting harmful content, send a report to Discord's support team.[304]

19.4 Twitch

Twitch, currently owned by Amazon, is a live-streaming platform where users can watch individuals around the world play video games live, while interacting with other viewers or host their own live-streams. While the platform is traditionally used by gamers, it can also be used to view live and recorded broadcasts covering topics like music, food, travel, talk shows, and more.[305]

19.4.1 Child Controls

Twitch is aimed at users over the age of 13. Those under 18 may only use Twitch if their parent or guardian agrees to Twitch's terms of service. Twitch does not offer a filtered service, nor controls those parents can use to limit a child's viewing time or the number of channels they can watch. Twitch streamers who consider their content can enable content warnings on their streams.

19.4.2 Twitch Strangers

A stranger is noted to be anyone who is not your friend, someone you follow, someone you subscribe to, one of your mods or one of your editors.

19.5 Twitch Privacy Choices

To find Twitch's privacy settings, open the **Account Settings**, click on your profile picture in the top-right corner, then click **Settings**. Once in **Settings**, go to the **Security and Privacy** tab and at bottom you will find the **Privacy** section.[306]

19.5.1 De-Linking Accounts

You can de-link your twitch account from other services (such as Blizzard Battle.net, Steam and League of Legends). This will prevent Twitch from sharing account information and user-related data. To do so, go to the **Connections** tab in your **Settings**. You are also able to revoke any authorizations to share your data with an Extension here.

19.5.2 Blocking Whispers from Strangers

Twitch whispers are a way for users to interact privately in a public group chat. By typing "/w" into a chat, followed by the username, only that user will see your message in the group chat. Blocking whispers from strangers can be done by toggling this choice on and off in the **Settings and Privacy** tab. This blocks whispers unless you whisper to them first.[307]

19.5.3 Blocking Gifts

To block the receiving of gifts from channels you do not follow, go to the **Security and Privacy** tab in **Settings**. Toggle the option to the off position.

19.5.4 Blocking Individuals

Within the **Security and Privacy** tab in **Settings**, you can view a list of users that you have blocked. To access this list, click **Show Blocked Users**. From there you can search for users, unblock users, and block added users as needed.[308]

- To add a user, enter their username into the search back and click **Add**.
- You are also able to click the individual's username, click on the three dots in the card that opens, and select **Block**.
- Finally, you are also able to type "/ignore<username>" in the chat to block someone.

19.5.5 Opt Out of Ad Tracking

You can opt out of Ad Tracking on Twitch under the **Privacy** settings on your mobile device.[309]

19.6 FACEBOOK

Facebook is a social networking website where users can post comments, share photographs, and post links to news or other interesting content on the web, chat live, and watch short-form video. Shared content can be made publicly accessible, or it can be shared only among a select group of friends or family, or with a single person.[310]

Facebook's business model relies upon selling targeted advertising to you based on the personal information you share with it via its online social media services.[311] [312]The following techniques can help mitigate any personal risk you assume by using these services.

19.6.1 Standalone Email Addresses/Phone Numbers

Use a standalone email address that is not linked to any other account beyond Facebook. It is also recommended that you use a separate mobile number as well if possible.

19.6.2 Mobile Phone/Web Browser Settings

It is recommended that you ensure that your mobile phone and web browser privacy settings are properly configured.

- To ensure this, please go through and apply guidance on these topics elsewhere in this document. To do so please see Sections 3.7.1 and 3.7.2.

19.7 Facebook Account Settings

19.7.1 Password Protection

Create a Facebook password different from the passwords you use to log into other accounts. For added tips, visit **URL**.[313] You can also test any sample password you choose at the following **URL**.[314]

19.7.2 Login Notifications

Facebook will send you a notification if someone tries logging into your account from a new device or browser.

- To learn more, visit **URL**.[315]

19.7.3 Login Approvals

Facebook will prompt you enter a special security code (*two-factor authentication*) each time you try to access your Facebook account from a new computer, phone, or browser.

- To learn how to turn on Login Approvals, visit **URL**.[316]

19.7.4 Trusted Contacts

Trusted contacts are friends you can reach out to if you ever need help getting into your Facebook account.

- Once set up, if you are unable to access your account, your trusted contacts can access special, one-time security codes from Facebook via a URL.
- You can then call your friends to get the security codes and use those codes to access your account.
- To set up your trusted contacts, visit **URL**.[317]

19.7.5 Login Location And Device Check

The **Where You are Logged In** section of your Security Settings shows you a list of browsers and devices that have been used to log in to your account recently.[318]

- You will also see the choice to End Activity and log yourself out on that computer, phone, or tablet.
- To review your active sessions and log out from unused browsers and apps, visit **URL**.[319]

19.7.6 Customize Notifications

You can adjust what Facebook activity you are notified about and how you are notified.

- For more details, visit **URL**.[320]

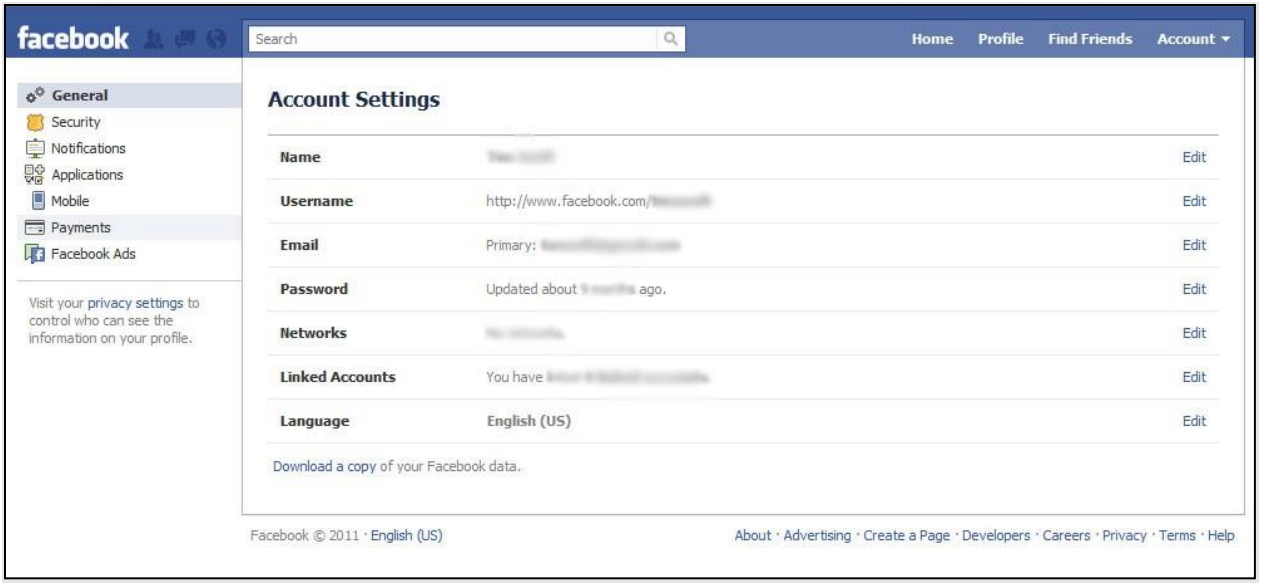


Figure 3. Facebook Account Settings.

19.8 Facebook Security Checkup

Use Facebook's Security Checkup to review and add more security to your account.

- To start your own Facebook Security Checkup, visit **URL**.[321]

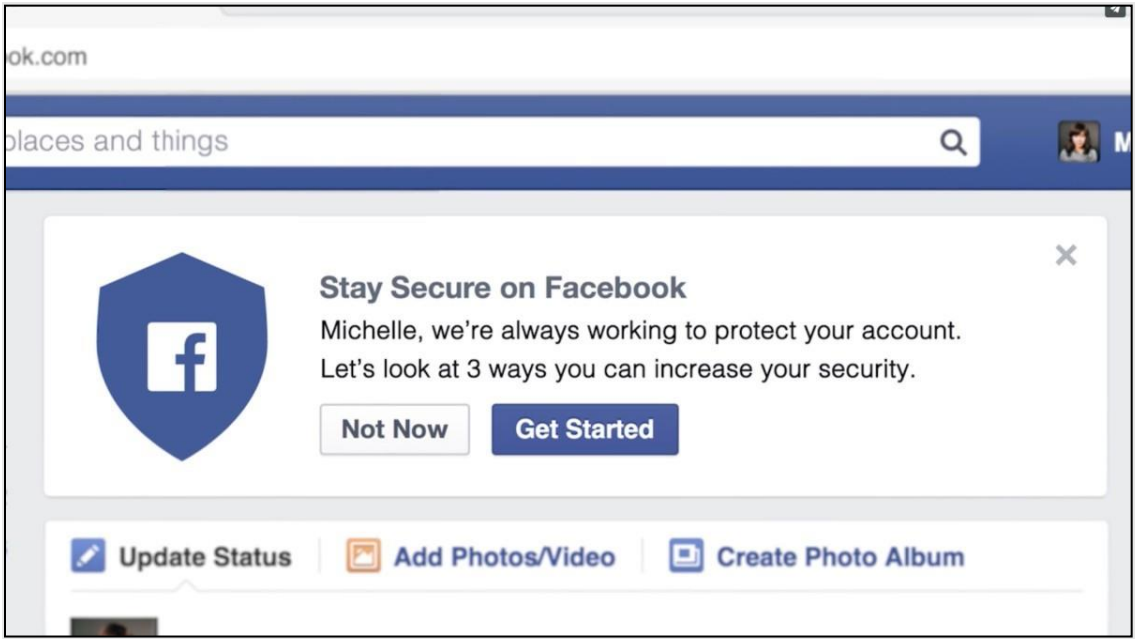


Figure 4. Facebook Security Checkup

19.9 Facebook Privacy Settings

19.9.1 Select Your Audience

Whenever you update your status, share photos, or post any information on Facebook, you can select who sees what you share through the audience selector tool.[322]

- This tool allows you to decide who sees what you share.
- The Custom option can be used to be as specific as you want for who can and cannot see something.[323]
- Facebook's help page will remind you ***when you post to another person's Timeline, that person controls what audience can view the post***. ***Additionally, anyone who is tagged in a post may see it, along with his or her friends.***
- To learn more about selecting audiences, visit the following **URL**.[324]

19.9.2 Review And Approval

There are two options within the Timeline and Tagging Settings for reviewing content that is tagged.[325]

- The first choice allows you to approve or dismiss posts that you are tagged in before they appear on your Timeline.
- This automatically applies to posts where you are tagged by someone you are not friends with, but you can choose to review all tags by turning on the timeline review.
- The second choice allows you to approve or dismiss tags people add to your posts.
- When you turn this on, a tag someone adds to your post will not appear until you approve it.
- To learn how to enable tag reviews, visit the following **URL**.[326]

19.9.3 Search Engine Visibility

- If you do not want search engines to link to your profile, you can adjust your Privacy Settings.
- However, some information from your profile can still appear in search engine results because it is information you shared to a Public audience or posts and comments you shared on Pages, Public groups, or the Community Forum section of the Help Center.
- To learn more, visit **URL**.[327]

19.9.4 Location Settings

Your location can be shared in many ways: with apps, by checking-in, via private messages, or by someone else tagging you.[328]

- It is important to consider when you share your location and with whom and to take measures to protect your location when possible.[329]
- To learn more about location privacy on Facebook, visit **URL**.[330]

19.9.5 View As Feature

You can see what your profile looks like to other people by using the View As tool.

- To learn more, visit **URL**.[331]

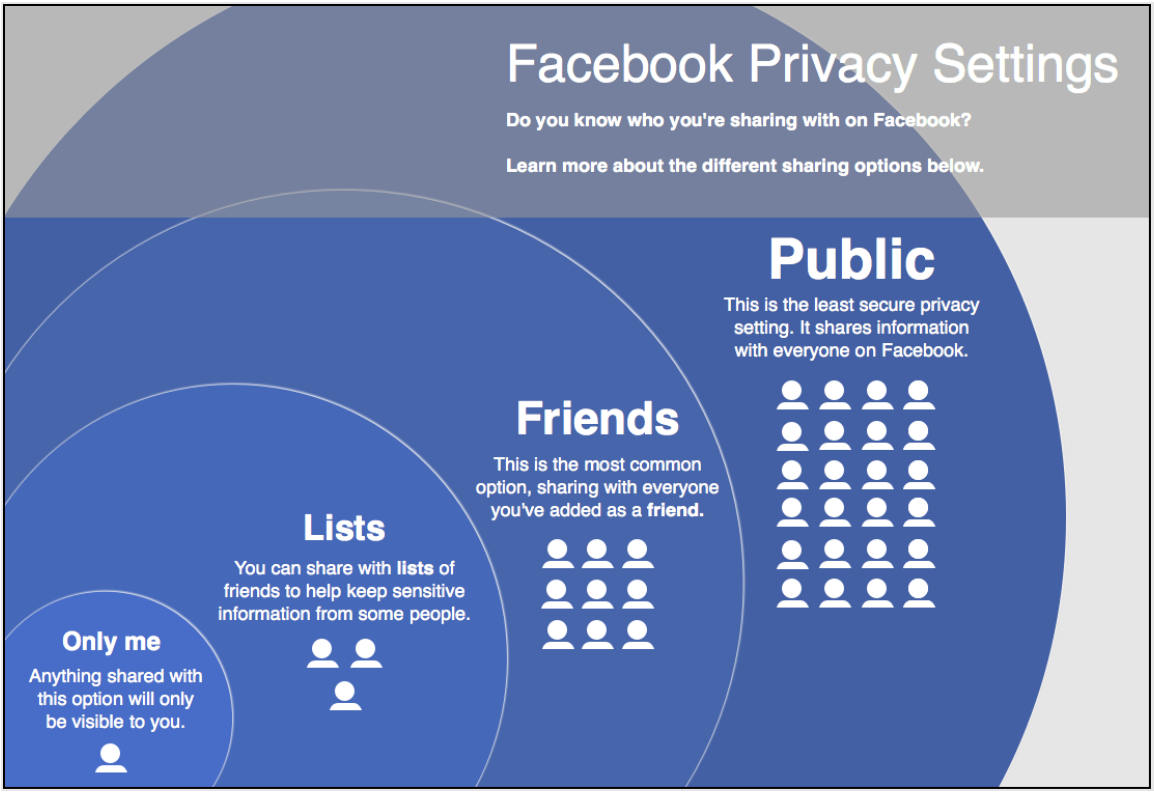
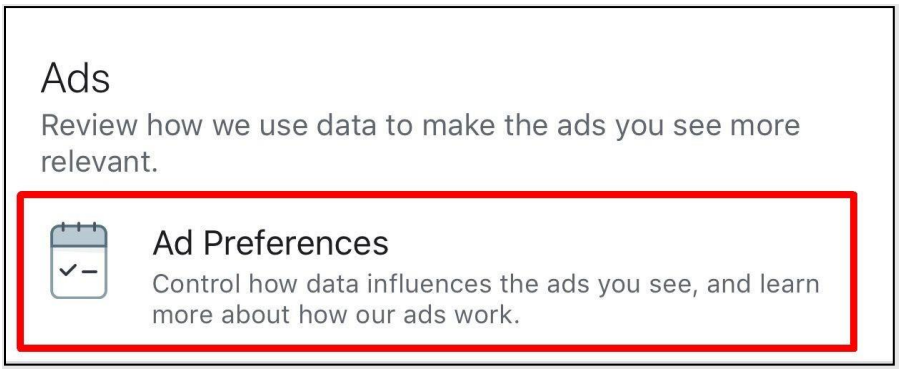


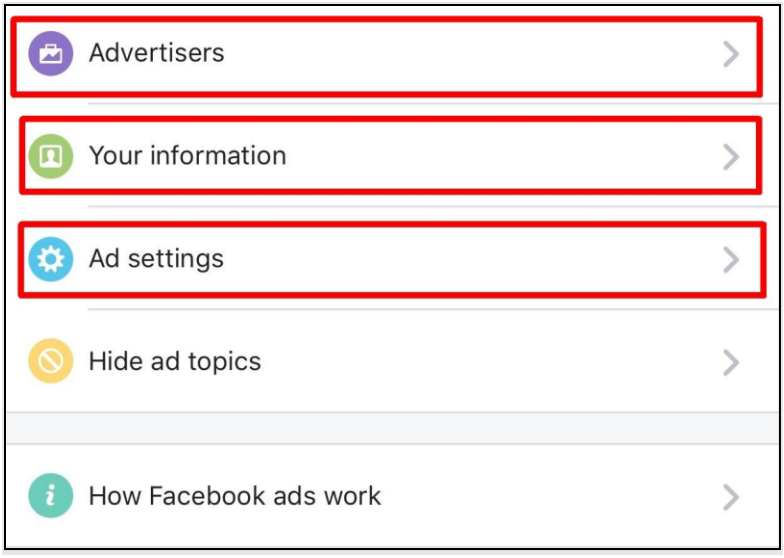
Figure 5. Facebook Privacy Settings

19.9.6 Disabling Advertising Features

Go to your Account Settings and enter the section for Ad Preferences.[332]

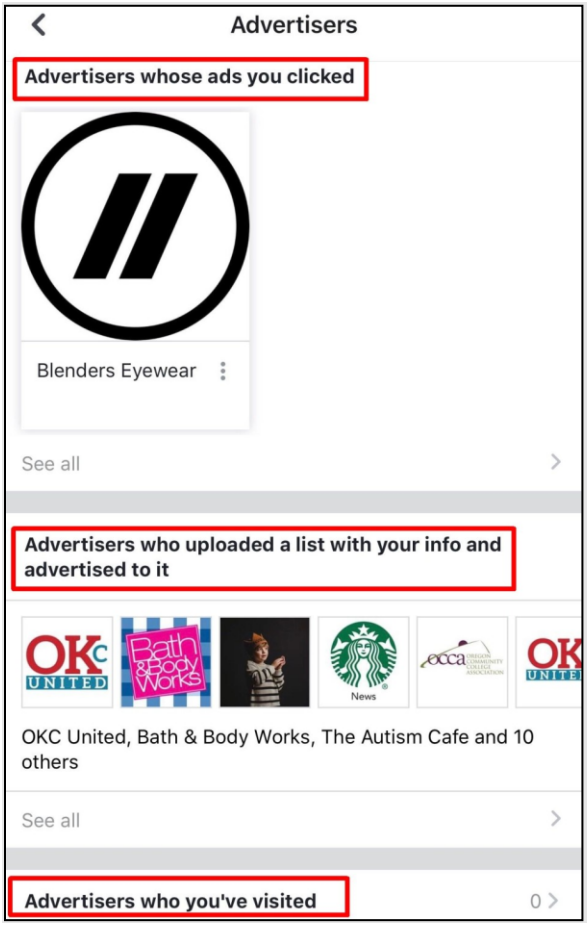


Then, enter each section **Advertisers**, **Your Information**, and **Ad Settings**.



19.9.6.1 Advertisers

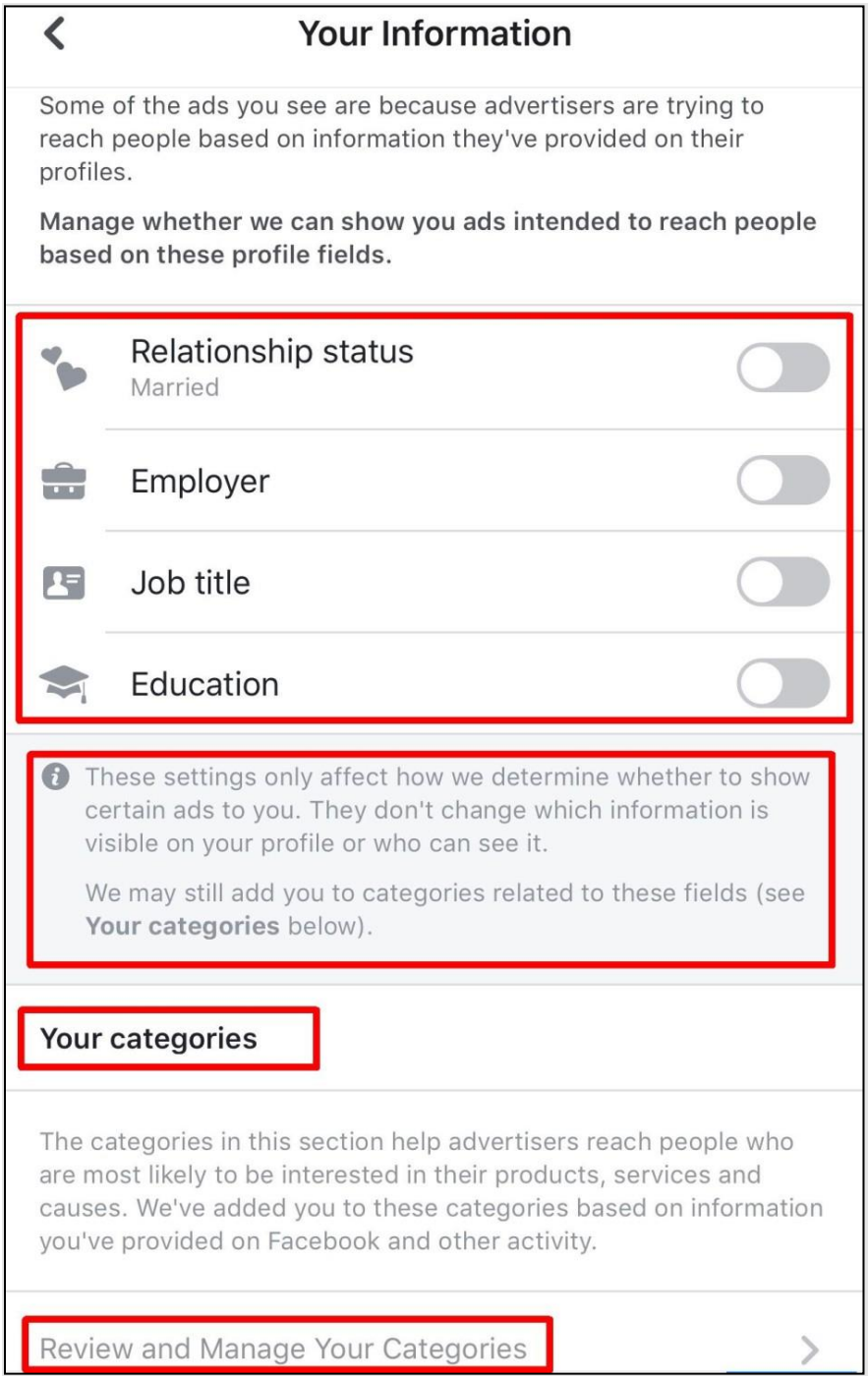
Your Facebook account will have the same sub sections as highlighted below. They will educate you how Facebook already used your information for its advertising purposes.[333]



19.9.6.2 Your Information

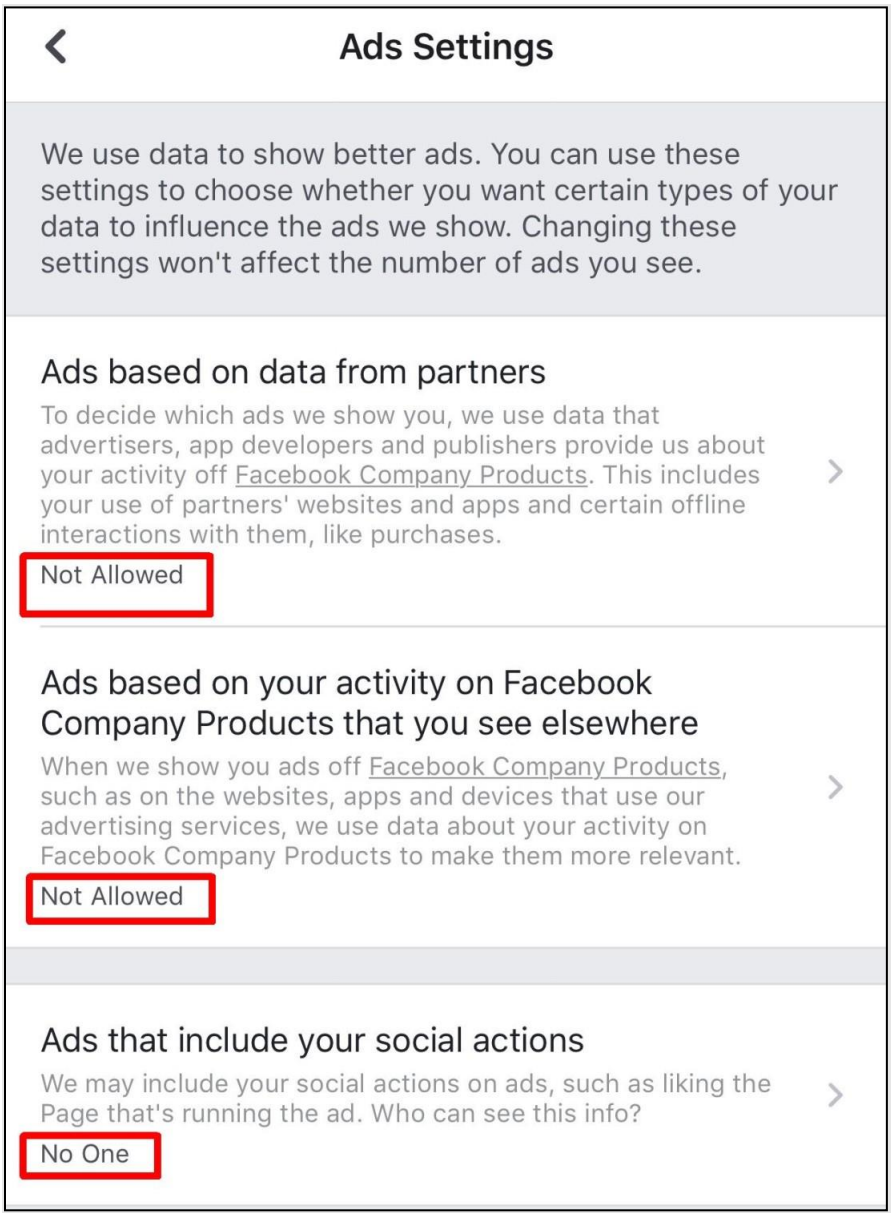
Everything in this section is available to how Facebook serves advertising to you and your management of it ***does not*** affect how Facebook profile looks.

- Pay close addition to the **Review and Manage Your Categories** section; you may have Wi-Fi and Phone settings in it, which you can opt out of as well.



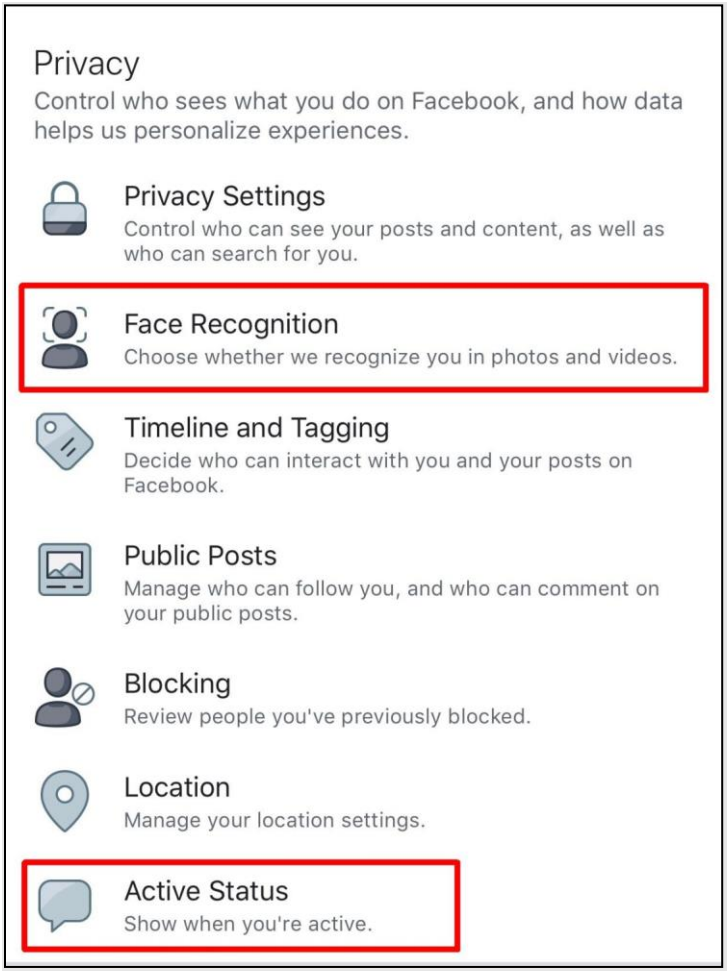
19.9.6.3 Ad Settings

Disable all Ad Settings under the sections entitled ***Ads based on data from partners***, ***Ads based on your activity on Facebook Company Products that you see elsewhere*** and ***Ads that include your social actions***.



19.9.7 Facebook Facial Recognition And Active Status

- Facebook describes facial recognition as "*Our technology analyzes the pixels in photos and videos, such as your profile picture and photos and videos that you have been tagged in, to calculate a unique number, which we call a template. We compare other photos and videos on Facebook to this template and if we find a match, we will recognize you. If you are untagged from a photo, or video, information from those untagged photos and videos is no longer used in the template. If your face recognition setting is set to off, we delete the template."* in their help center post at the following **URL**.[334]
- Disabling active status allows you to run on the service private from other users and Facebook friends.



19.10 MANAGING YOUR FACEBOOK COMMUNITY

19.10.1 Friend Requests

Facebook is where so many of us connect with people we know personally, like friends, family, classmates, and coworkers. Facebook is based on authentic identities, where people are who they are in the real world.

19.10.2 Do Not Use Your Full Name

This is one of the fastest ways to get into someone's life so you might as well make it harder for someone to find you if they get a hold of your personal information or use Facebook to gauge your life even in new social circles.

- Unfortunately, as Facebook notes, some individuals use tactics such as impersonating a friend to gain access to personal information.
- If you receive a friend request from someone you are already friends with, ask if they sent the new request before accepting it.
- If they did not create it, report the impersonating profile to Facebook.
- If you want to meet new people through Facebook, try connecting with Pages and groups that interest you.
- You can also choose to limit who can see your friend list if you are worried about your friends and family being contacted by someone.
- To learn more about adding friends and friend requests, visit **URL**.[335]

19.10.3 Unfriending

To unfriend someone, go to that person's profile, hover over the Friends button at the top of their profile and select Unfriend.

- If you choose to unfriend someone, Facebook will not notify the person, but you will be removed from that person's friends list.
- If you want to be friends with this person again, you will need to send a new friend request.
- To learn more about removing friends, visit **URL**.[336]

19.10.4 Blocking

- Blocking a person automatically unfriends them and blocks them so they can no longer see things you post on your profile, tag you, invite you to event or groups, start a conversation with you, or add you as a friend.[337]
- Blocking is reciprocal, so you also will not be able to do things like start a conversation with them or add them as a friend.
- When you block someone, Facebook does not let them know you have blocked them. To learn more, visit **URL**.[338]

19.10.5 Reporting

Any type of content can be reported to Facebook. Facebook's Community Standards explain what type of content and sharing is allowed on Facebook.

- When something is reported to Facebook, a global team reviews it and removes anything that violates these terms.
- To learn how to report and what happens when you click report, go to the following **URL**.[339]

Figure 6. Facebook Notifications Center

19.11 FACEBOOK MESSENGER

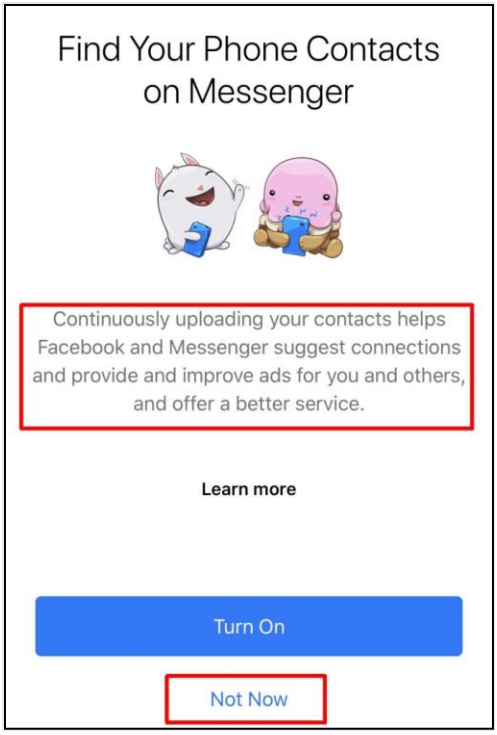
Facebook Messenger is a free messaging app and web-based platform that enables Facebook users to conduct instant message-based conversations with Facebook friends. Originally developed as Facebook Chat in 2008, the company updated the service and rebranded as Facebook Messenger in 2011.
Users of Facebook Messenger can send messages and exchange photos, stickers, audio, and files, as well as react to other users' messages, interact with bots, and conduct voice or video calls.
While Messenger was once limited to Facebook users only, it now powers conversations within Facebook, Instagram, Portal, and Oculus VR.[340]

19.11.1 Disabling Facebook Messenger From Automatically Syncing Your Contacts

19.11.1.1 If You Are Installing the App

Pay close attention to what prompts appear on your Mobile Phone as you install Facebook Messenger. After you have installed the App, you will begin setting up your profile based on existing Facebook information or whatever information you have provided.

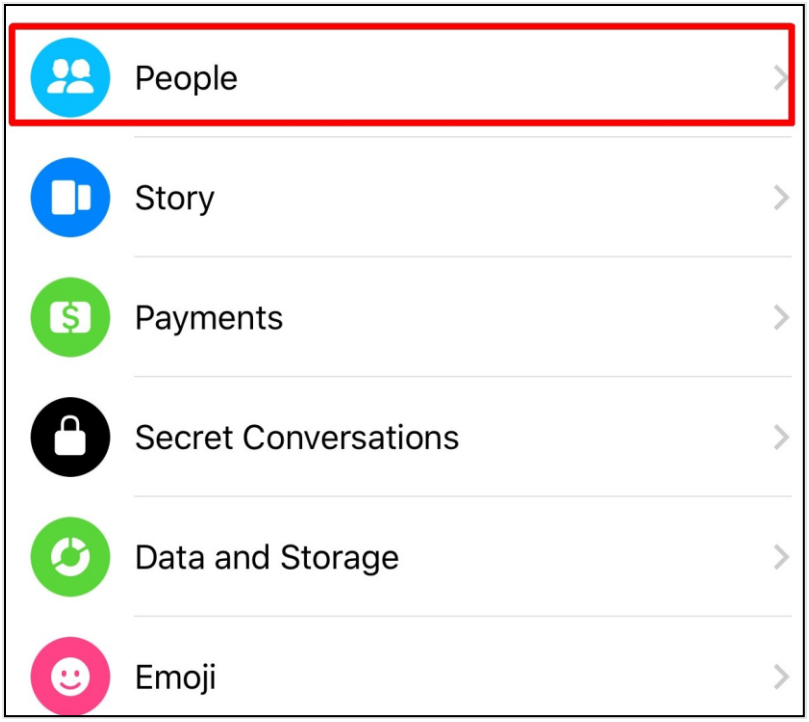
- You will then see a prompt on your screen with two animated creatures. If you read the dialogue carefully (as highlighted in the graphic), you will see the text, which shows **"Continuously uploading your contacts helps Facebook and Messenger suggest connections and provide and improve ads for you and others and offer a better service."**
- Make sure you click on **'Not Now'**.
- This will prevent Facebook Messenger from uploading your contacts into the Facebook ecosystem.

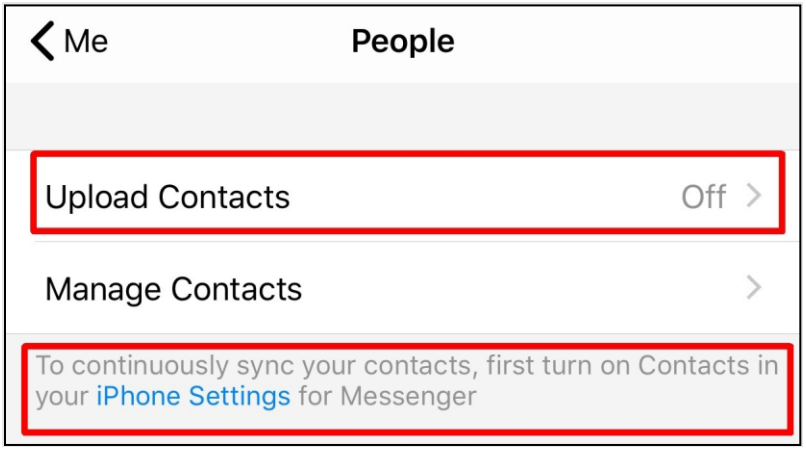


19.11.1.2 If The App Is Already Installed

You were unaware that enabling the feature discussed above actually uploaded your contact list from your Mobile Phone into the Facebook ecosystem so now you would like to go back, disable the setting, and now retroactively remove your contacts from Facebook Messenger.

- Here is how you disable the setting to stop continuously synchronizing your contacts with Facebook Messenger as well as remove them from Facebook's ecosystem.
- Launch the Facebook Messenger app from your Mobile Phone or Personal Device and go to the home screen.
- Look for the photo icon at the top left-hand corner of the screen and Tap on it.
- Now tap on '**People**' within the 'Preferences' section **(as highlighted in the graphic below).**
- Now tap on **'Upload Contacts'** and ensure you have the setting adjusted to '**Off**'.

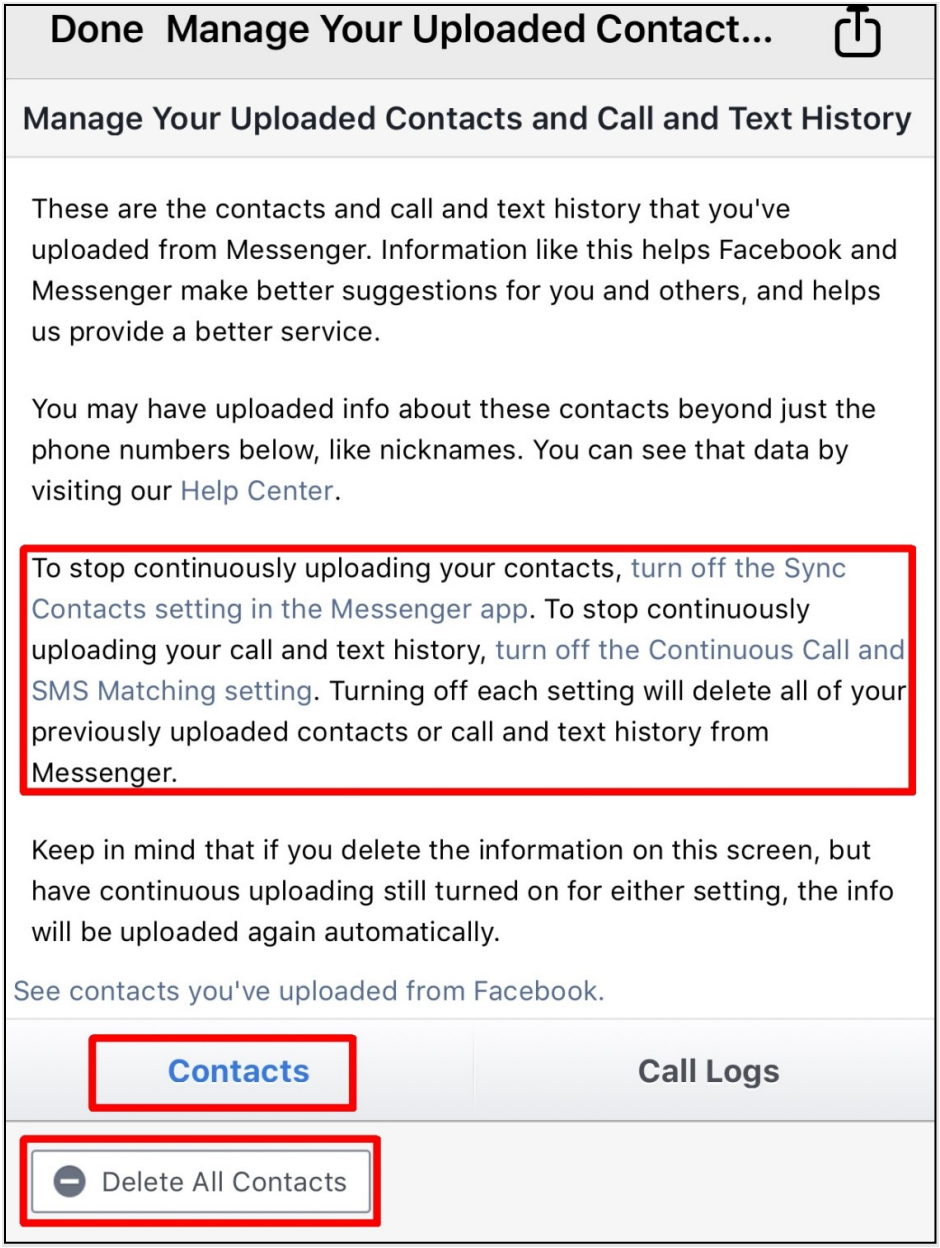




19.11.1.3 Stopping Facebook Messenger From Automatically Syncing Your Contacts (If the App Is Already Installed)

According to Facebook at the following **URL** when you turn off contact uploading, the contacts you have uploaded to Messenger will automatically be removed.[341]

- You can also go to the **Manage Your Uploaded Contacts** screen and tap **Delete All Contacts > Delete All Contacts** to delete these contacts. To stop your contacts from being uploaded again, you will need to turn off contact uploading on any devices where you are using the Messenger app.



19.11.2 Additional Privacy Settings

You can control your privacy in Messenger by choosing who can see your active status, choosing your Story audience, using secret conversations and more. Here are some ways to control your privacy in Messenger.

19.11.2.1 Control Who Can See When You Are Active

Active Status shows your friends and contacts when you are active or recently active on Facebook or Messenger.

- The following link will instruct you on how to **control your active status in Messenger**.[342]

19.11.2.2 Control Chat Lists

If someone who you are not connected with on Facebook sends you a message, you will receive a connection request.

- The following link will instruct you on how to **control who can start a new chat with you in Messenger**.[343]

19.11.2.3 Secret Conversations

Secret conversations in Messenger are end-to-end encrypted and can only be read on one device of the person you are communicating with. The following link will instruct you on how to use **secret conversations in Messenger**.[344]

19.11.2.4 Clear Your Search History

Facebook Messenger allows users to edit or clear their search history in Messenger. The following link will instruct you on how to **clear your search history in Messenger**.[345]

19.11.2.5 Remove Sent Messages

Facebook Messenger allows users to permanently remove a message that you have sent for everyone in the chat, or just for yourself.

- The following link will instruct you on **how to remove a message** within Facebook Messenger.[346]

19.11.2.6 Customize Story View

You can control who can and cannot see your story.

- The following link will allow you to **choose who can see your story in Messenger**.[347]

19.12 INSTAGRAM

Instagram is a free social networking service built around sharing photos and videos. It launched in October 2010 on iPhone first and became available on Android in April 2012. Facebook bought the service in April 2012 and has owned it since. Like most social media apps, Instagram allows you to follow users in which you are interested. This creates a feed on your homepage, showing recent posts from everyone you follow. You can like posts, comment on them, and share them with other people.[348]

19.12.1 Instagram Start Screen

The graphic of Instagram's start screen can be found at the following link.

19.12.2 Open The Camera

When you are on the home tab, you can tap the "camera" icon in the top left-hand corner to start adding photos and videos to your Instagram profile.

- NOTE: You will need to allow Instagram to access your camera and microphone before you can use this feature.

19.12.2.1 Direct Messages

The "paper airplane" icon in the top right from the home tab will get you access to your direct messages.

- Here a user can view messages from people as well as create direct messages to send to your connections.

19.12.2.2 The Home Tab

This is the default view when you open the Instagram app. It is also, where the media, images, and stories from the people you are following will appear.

- From the home tab, you have access to add photos and/or videos to your feed, access your direct messages, search, connect and access your profile settings.

19.12.2.3 The Search Page

The magnifying glass will take you to the **"Search"** page.

- From here, you can search for accounts, keywords, hash tags, and topics simply by typing in the **"Search"** bar at the top of the screen.

19.12.2.4 The Camera Page

By clicking on this button, you will see your phone's camera popup. From here, you can either choose to add a photo or video from your camera roll (already on your camera) or choose to take a new one.

- NOTE: You will need to allow Instagram to access your camera and microphone before you can use this feature.

19.12.2.5 Account Activity

The "heart" icon will take you to your account activity page.

- This is where a user can see comments, likes, shares, and follows for your account, as well as the people you are following.

19.12.2.6 Profile And Account Settings

A user can access their own profile and account settings by tapping on the little icon that looks like a person.

- Once on this tab, a user can choose to add latest photos and videos, edit your profile and more once again.
- While on this page, tapping the 'hamburger icon' in the top right will slide out more options where you can view your **"saved posts"**, or access the **"discover people"** functionality to connect with your friends from Facebook, or access Facebook directly.

19.13 Instagram's Privacy and Safety Center

If a user need added help in understanding the wide-ranging settings Instagram offers you as a user for safety and reporting threatening activity, the following Instagram help center **URL** is extremely informative.[349]

19.13.1 Privacy Settings

The following privacy settings should be enabled to make a user safer while they are using the platform as well as ways you can reduce your Digital Exhaust.

19.13.1.1 Private Profile

This is the most popular privacy setting and one you should enable right away. By default, Instagram accounts are public, meaning; anyone on Instagram can view your photos, like and comment on them.[350]

- Instagram gives you a choice to make your profile private. When you have a private profile, only your followers can see your published photos and stories.
- This setting does not change your viewing method, as you can still see other public profiles' photos and stories.
- To make your profile private, first open the Instagram app and go to the profile screen. Then tap on the three-dot icon at the top-right corner to open Settings in case of Android phones. On an iPhone, tap on the gear icon.
- Under **"Settings"**, tap on **"Private account"** and turn it on. You must also tap on Account privacy and enable the setting **"Private account"**.

- It is unknown why Instagram has kept the same setting in two places. Per Instagram, business profiles are not able to make their accounts private.
- If you want to make your business account private, first switch back to a personal account.

19.13.1.2 Removing Followers

When a user makes an Instagram profile private, there will be many people in your Followers list that you do not want there. Previously, you had to block such users, but Instagram has changed that setting now.

- It is not necessary for you to have a private profile to remove followers, you can do this even if you have a public profile. According to Instagram, removing specific followers will not let them know about being removed.
- To remove Instagram followers, go to your **"Profile"** and tap **"Followers"**. You will see the three-dot icon next to every follower.
- Tap on it for the follower you would like to remove and select **"Remove"** on the pop-up screen. If you would like added screenshots, the following link is helpful.

19.13.1.3 Turning Off Your Activity Status

In 2018, Instagram launched an Activity status feature. It shows the last time users were active on Instagram and with whom they had direct conversation. In addition to your activity, Instagram also introduced the online status indicator.[351]

- When a person is online, you will see a green dot next to their username in Direct Messages (DM). Per Instagram, here are the steps to turn them off.
- Go to your profile and tap the three-dot icon or the gear icon. Scroll down and tap on **"Activity status"**. On the next screen, disable **"Show activity status"**. This will turn off activity status and green dot both.

19.13.1.4 Blocking Comments

Sometimes when people do not like a picture or video that you posted, they resort to trolling you in the comments. Instagram gives you the choice to turn off their comments.

- You can do this for all posts from the general **"Settings"** and even for an individual post. Per Instagram, here is how you what you need to do to stop comments on all your Instagram posts.
- On your profile, tap on the three-dot icon to go to **"Settings"**. Under **"Settings"**, tap on **"Comment controls"**.
- Then you will get two options: **"Allow Comments from"** and **"Block Comments from"**. You can use the first choice to white filter the comments. Meaning, only the people that you add here will be able to comment on your posts.
- On the other hand, when you block people from commenting, everyone else except these users will be able to comment.
- To turn off comments for an individual post, open the post and tap the three-dot icon at the top-right corner.
- Select **"Turn off commenting"**.
- You can also enable the setting **"Hide offensive comments"** as well as the **"Manual filter"** option.

- If you need to report offensive or abusive behavior, Instagram provides you with instructions on how to do so at the following link.

19.13.1.5 Stopping Direct Messages (DM)

Everyone on Instagram can message you, whether they follow you or not. However, messages from people other than your followers are kept under a separate folder (Requests) in DM. While Instagram does not let you stop DMs for normal messages, you can restrict DMs for stories.[352]

- Instagram offers three settings for message replies in stories: **"Everyone"**, **"People you follow"**, and **"Off"**.
- Here is how to set it. Open Instagram Settings by tapping the three-dot icon (Android) and gear icon (iPhone) on the profile screen.
- Next, tap on **"Story controls"** and under **"Allow message replies"**, select the preferred option.

19.13.2 Privacy Settings & Information Link

If you need added help in understanding the wide-ranging settings Instagram offers you as a user, the following Instagram help center link is extremely informative.[353]

19.13.3 Disable "Resharing Posts To Stories"

If you have a public profile, people can reshare your posts on their stories along with your username. While some people may not have an issue with it, here are the steps Instagram provides you the to turn this feature off.

- Open your Instagram Settings and scroll down and tap "Resharing to stories" and ensure you have disabled this setting.

19.13.4 Hide A Story

Instagram offers different privacy settings for posts and stories. While you cannot change the privacy of individual posts, you can customize the privacy of your stories which will allow you to hide stories from specific followers.

- To do so, launch Instagram Settings and tap on **"Story Controls"**. Select the followers from whom you want to hide stories under the **"Hide story from"** option.
- A couple important Privacy tips for you on sharing Instagram stories, Private posts you share to social networks may be visible to the public depending on your privacy settings for those networks.
- Instagram offers an example at the following link that a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your Twitter posts. This is a prime example of how your Digital Exhaust can pop up in ways you least expect it.

19.13.5 Approve Tagged Posts

Instagram has a separate section for tagged photos and videos. When a person tags a user, it will automatically be added to their profile, so it is better to approve tagged posts first. Once a user approves them, only then they will be added to your profile.

- To enable this setting, continue to Instagram Settings and tap on **"Photos of you"**. From here you can disable the setting **"Add Automatically"**. If you would like to hide a photo or video you have been tagged in, the following link from Instagram will provide you steps to do so.

19.13.6 Clear Instagram's Search History

If you often search for a person or a hashtag, it will appear under the search tab in Instagram.[354]

- To clear your search history, open Instagram Settings and tap on **"Search history"**.
- Then on the next screen, tap on **"Clear search history"**.

19.13.7 Photo Metadata

The start of each photo presents unique Digital Exhaust which when left unchecked, can be exploited by savvy threat actors.

- It is recommended that you remove any EXIF data so you do not hand it to a third party should a data breach occur even if it is stripped from social media platforms or in texting exchanges.
- In addition, it is recommended that you turn off geotagging by default.
    - NOTE: When you turn off geotagging, it only applies to photos taken after you have turned off the location feature.[355]

19.13.8 Location Settings

It is recommended a user NOT showing your location when posting.

- If you do not understand how Instagram's Location Tags work, the following link is extremely informative.
- If you need a hand locking own your Location data, check out the following **URL** which outlines how your personal device(s) collect and track your daily location and ways you can increase your awareness of this issue with all Apps or Devices you use.

19.13.9 Syncing Contacts And Finding People

When it comes to synchronizing your contacts from your Mobile Device to Instagram, It is HIGHLY DISCOURAGED to do so. As Instagram is part of the Facebook ecosystem, the Guide has already covered the dangers of synchronizing contacts.

- If you need added help understanding how Instagram works with syncing contacts and finding people, the following Instagram help center **URL** is extremely informative.[356]
- Additionally, if you would like information on how to disconnect your Instagram account from another social network, the following **URL** is helpful.[357]

19.13.10 Resources For Parents

The following **URL** will be immensely helpful for parents of children who use Instagram.[358]

- Instagram has a simple interface that is easy for unaccustomed users to understand intuitively, no matter their age, there are several Privacy settings that are highly recommended a user enable.

19.14 LINKEDIN

LinkedIn is the world's largest professional network on the internet. You can use LinkedIn to find the right job or internship, connect and strengthen professional relationships, and learn the skills you need to succeed in your career. You can access LinkedIn from a desktop, LinkedIn mobile app, mobile web experience, or the LinkedIn Lite Android mobile app.[359]

19.14.1 Social Engineering On LinkedIn

LinkedIn does not require any authorization for you to associate your account with a company. can expose a user to reputational risk and trust issues if malicious actors perpetrate fraud, troll other accounts, or otherwise use the false pretense of being one of your employees to do harm to others. With a false LinkedIn identity, threat actors can readily create malicious trust relationships with targeted users. With a fake LinkedIn account, a threat actor can get individuals to unwittingly expose other sensitive information.[360]

19.14.1.1 Detecting Fake LinkedIn Accounts/Personas

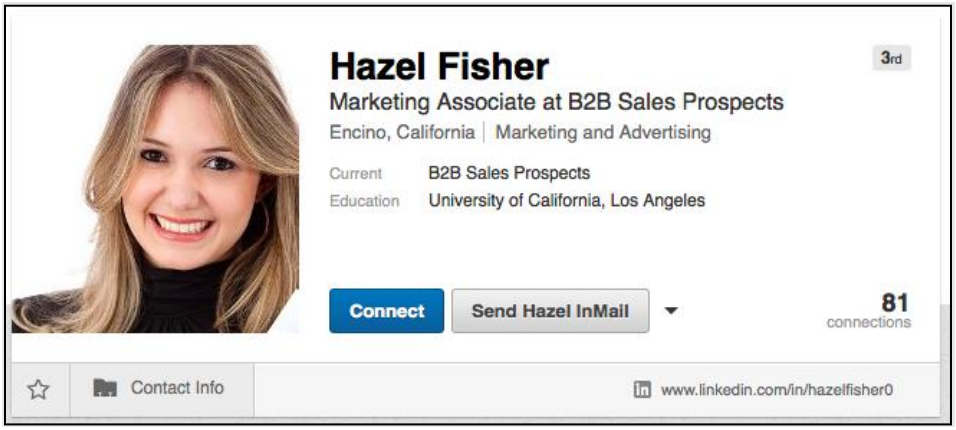
This section will give tips for how to spot fake or “doppelgänger” LinkedIn accounts. This is critical because connecting with a fake LinkedIn profile can give cyber criminals or Advanced Persistent Threat actors access to important and powerful information about you, such as details about your history, company, and professional contacts.[361], [362]

- That information can be used to create detailed and believable phishing campaigns and other financial swindles.[363]
- In short, beware of LinkedIn accounts with fake photos, incomplete profiles, limited connections, fake names, poor spelling, and grammar, and/or suspicious work history.

19.14.1.2 Fake Photos

Model-quality photos often go with many Fake LinkedIn profiles.

- If you are suspicious about a photo, there is a straightforward way to check its authenticity. Simply do a reverse image search using **TinEye**, **Bing's Visual Search** or **Google’s Reverse Image Search**.
- These search engines will show you where, if any place, the same image has been used previously online.



19.14.1.3 Incomplete Profiles

One key indicator of fake LinkedIn accounts is the lack of any information about the individual. If there is information, it is often in the form of mostly generic statements that lack any specificity in the summary and experience sections.

- Conversely, genuine profiles belonging to real people typically include a mixture of personal details, such as causes, volunteering, hobbies, education, recommendations, and the use of the first person when writing the 'Summary' or 'Experience' sections.
- Many fake profiles used for swindles do not bother to add personal information and keep detail to a minimum.
- Most people also personalize their custom LinkedIn URL while false accounts will not as they are created quickly and without tremendous attention to detail.
- This may not be the case for more sophisticated Cyber criminals or Advanced Persistent Threat actors.

19.14.1.4 Limited Connections

Genuine profiles typically have a mixture of people and profiles among its connections.

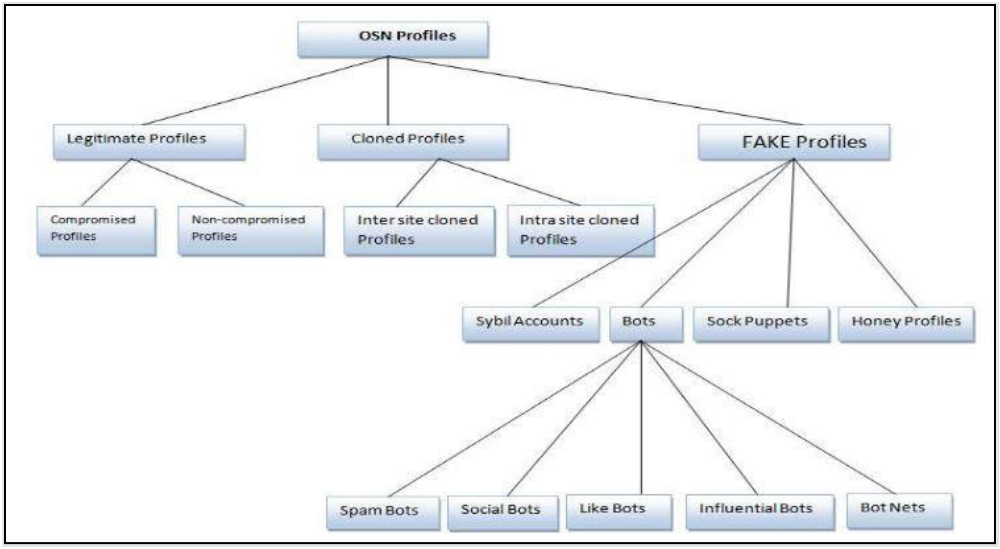
- Fake profiles may have connections with all the same or all opposite gender people with fake-looking profile pictures.
- Fake profiles can range from a few to several hundred connections, as well as a handful of skill endorsements.
- They also usually belong to several groups and follow a couple of companies and influencers.
- Check out mutual connections from a connection request, or better yet, message your connections directly to see if you can confirm an individual's identity prior to connecting to their profile.

19.14.1.5 Fake Names Or Doppelgangers

Threat actors may create fake names or doppelgänger accounts to help their threat activities.

- Accounts created in this may use generic names or that of a famous person, like an actor, actress or television personality.
- Some scammers will use the name of a more obscure actor or actress that would not be as known to most of those on LinkedIn.
- Threat actors may also create accounts that impersonate a legitimate person's account. These accounts are doppelgangers, and their users try to assume a legitimate connection's identity as best as they can.
- These doppelganger accounts are often 3rd degree connections. To protect against this, run the account name in LinkedIn's search function to see if they have more than one account.
- If so, you may have showed their doppelgänger or found the true account and uncovered that whomever you are interacting with is the doppelganger.
- If you can, block the illegitimate account(s). This prevents the threat actor from viewing your profile, trying to follow your account on LinkedIn, and from delivering any type of malware to you through LinkedIn InMail.

More about doppelgänger accounts are available in the article "A Sneak Into The Devil's Colony-Fake Profiles in Online Social Networks" at the following **URL**.



19.14.1.6 Poor Spelling And Grammar

Many fake profiles include obvious errors like misspellings and poor grammar. Often, the first name is displayed in all capital or lowercase letters, which would not be common to see in a genuine profile.

19.14.1.7 Suspicious Work History

One of the most effective ways to detect a suspicious work history is to check a connection's work experience by looking for their current employer elsewhere online and see if the person with the suspect profile is, in fact, listed as working there.

19.14.1.8 Suspicious Connection Requests

Be sure to vet connection requests if they have content with languages unfamiliar to you. Use the **Google Translate App** at the following **URL** if you want to read what the profile says in any unfamiliar language.[364] On a mobile phone, take a screen shot and import it.

19.14.2 LinkedIn Privacy Settings

LinkedIn provides users with several privacy options.

- Review the following **URL** to better understand ***them*** then head over to begin controlling them.[365]
- You can control them at the **URL**.[366]

19.14.3 Settings & Privacy Page

The Settings & Privacy Page is organized into four tabs to help you easily view and change your account information, privacy preferences, ads settings, and communication notifications to include:

- **Account tab** - allows you to manage your account settings, such as adding email addresses, changing your password or language, and other account management options.
- **Privacy tab** - covers all privacy and security settings related to what can be seen about you, how information can be used, and downloading your data.
- **Ads tab** - enables you to control the information that LinkedIn uses to show you relevant ads by adjusting your account's ads settings.
- **Communication tab** - houses your preferences for how LinkedIn and other parties can contact you, and how often you would like to hear from us.

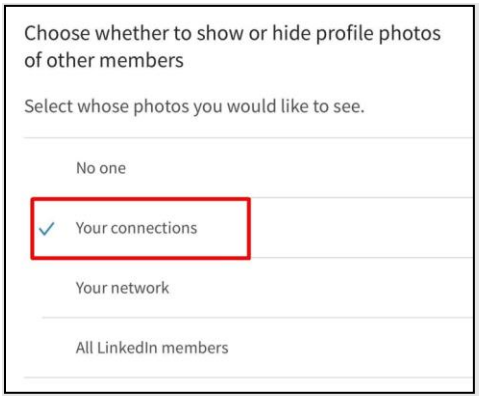
19.14.4 LinkedIn Account Settings

You can also check out the following information to learn more about some key settings you can manage through the Settings & Privacy page to include:

- **Changing Your Password**
- **Adding or Changing Email Addresses**
- **Adding and Removing Mobile Phone Numbers from Your Account**
- **Stopping or Changing Email Notifications**
- **Sharing Profile Changes with Your Network**
- **"Who's Viewed Your Profile" - Overview and Privacy**
- **Turning on Two-step Verification for Improved Security**
- **Setting push notification settings**
- **Viewing your groups**

19.14.4.1 Profile Photos On LinkedIn

You can suppress your profile photo from being displayed to everyone and only to people you confirm.



19.14.4.2 How Your Name Appears On Your Profile

LinkedIn allows you to control how people see your last name on the platform. Hide your last name from people not connected to your account.

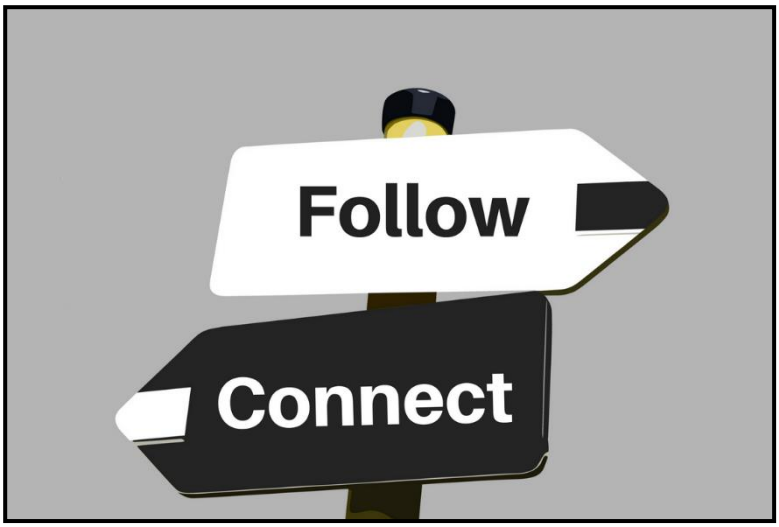
19.14.4.3 Reviewing Where Your Name Appears On Your Profile

Modify your account's custom URL on your LinkedIn profile to omit your full name.

- Also, it is recommended you do not openly post your resume online.
- It is also advised that you review any recommendations you receive and ensure your last name is controlled on them and any other personally identifiable information is not visible in them.

19.14.4.4 Follow Accounts Instead Of Connecting To Them

According to LinkedIn, *"Connections are members who connected on LinkedIn because they know and trust each other. If you are connected to someone, you will both be able to see each other's shares and updates on your LinkedIn homepages. You can also send messages to your connections on LinkedIn.* ***Following someone on LinkedIn allows you to see the person's posts and articles on your homepage without being connected to them.*** *However, the person you're following won't see your posts."*



- More is available at the following **URL**.[367]
- The Following feature is a valuable tool provided by LinkedIn. It enables sensitive and high-profile users to overtly control to whom their accounts connect.
- Users can always view a list of your followers on your profile page at the following **URL**.[368]
- They can also manage who can follow their updates at following **URL**.[369]
- Do this to ensure no suspicious or nefarious individuals are remotely viewing your LinkedIn profile.

19.14.4.5 Searching For People On LinkedIn

Assuming you controlled your account's last name and photo, it is more difficult for threat actors to spoof your LinkedIn account with a doppelgänger account.[370]

- Regardless, search your name in LinkedIn to look for any 3rd-degree connections who may be trying pass themselves off as the real you.
- The article at the following **URL** offers a great overview for how to search.[371]
- You can also perform Boolean searches on LinkedIn. Instructions for how to do this are available at the following **URL**.[372]
- Also, if you want a better understanding about how your network and degrees of connection work on LinkedIn, read the article at the following **URL**.[373]

19.15 SNAPCHAT

Snapchat markets itself as a social media platform on which sent images and messages are only available for a limited amount of time.[374] The time limit is set by each individual user.[375]

- A recipient, however, can still take a screenshot of sent photos or chats or use another device to take photos of any sent material (users are notified when their message has been screenshotted).
- Further, there are many other ways in which people can collect information about a Snapchat user particularly if that user does nothing to change their privacy settings.[376]

19.15.1 Start Screen

Opening the mobile Snapchat app immediately opens that device's camera. To navigate to other pages of the application either select another choice at the bottom of the screen or the yellow silhouette in the top left-hand corner to navigate to your profile page. The profile page looks like this:

- First, make sure that simply because someone has your phone number or email, they cannot search for you using that information on Snapchat. Instead, they would need your exact username. Selecting the gear icon in the top right corner of your profile page will navigate you to the settings page.
- Select **Mobile Number** then uncheck **Let others find me by using my mobile number**. Repeat the process for email. Now if a blocked caller tries to find you via Snapchat, it will be much more difficult.

19.15.2 Profile And Settings

This area allows users to access a variety of features to include using the two-factor authentication feature, turning off your location, managing target ads, controlling who contacts you, managing Snapchat's use of your contacts, and finally controlling who you share with.[377]

- To navigate to settings, go to the gear icon in the top righthand corner of your profile page.

19.15.3 Enabling Two-Factor Authentication

This feature means that when logging into Snapchat, users must enter an added code (sent via SMS) after the password.

- Someone would need to have both your password and your phone to access your account.

19.15.4 Location Sharing

To turn off your location, control who contacts you, and control who you share information with, navigate to Settings and scroll to the **WHO CAN** section.

19.15.5 Ghost Mode

Select **See My Location** to turn on Ghost Mode (no one can see your location) or you can customize the location settings to allow certain users to see your location.

19.15.6 Contact Accessibility

Select **Contact Me** to make sure only your friends can contact you.

19.15.7 Information Visibility

Select **View My Story > See My Location > See me in Quick Add** to control who can see your information.

19.15.8 Opting Out Of Targeted Ads

Go to **Settings > Additional Services > Manage**

19.15.9 Use Of Contacts

When you first use the app, Snapchat asks if you would like to synchronize your contacts.[378]

- At this point you can grant permission for the Snapchat app to access your contacts and make updates whenever you add a contact to your phone.
- If you originally allow Snapchat this access, you can change it later by unchecking **Sync Contacts > Additional Services > Manage > Permissions**
- Following the above recommendations can reduce a user's Digital Exhaust, however, following all these steps also reduces the usability of the app.
- Further, by not allowing Snapchat to synchronize with your contacts, you will have to manually search for someone in Snapchat to see if they have an account.

19.16 TIKTOK

TikTok (formally branded as musical.ly) is a freeware, cross-platform, short-form mobile video media application. TikTok uses a device's data plan or Wi-Fi to broadcast trending video media created by users. [379]

- The application is free to users and is supported by advertisements.
- TikTok users draw from a cadre of free tools to create content for sharing, as well as Livestream content that may use real-time filters.
- This application is used for mobile devices but also has workarounds for use in desktop computers.

19.16.1 TikTok Screen Management

TikTok supplies a Screen Time Management setting for a daily usage maximum (i.e., 40, 60, 90, or 120 minutes per day) that allows users the ability to pre-decide the daily time spent in the application.

- When the selected time is met, a password is needed to continue to use TikTok –presuming that a parent or guardian selects the required password or that the user will self-monitor the time limit.
- If you wish to limit time on the app, go to the **Digital Wellbeing** section of the Settings & Privacy page and use the **Screen Time Management** option to select your time limit.
- You can also set a pin code which will be used for both Screen Time Management and Restricted modes.

19.16.2 Making Your Account Private

- Launch the **TikTok** app.

- Open the **Me** tab in the bottom right **>** tap the three vertical dots in the upper right **> Privacy and Safety > Private Account**, if your profile is in Pro Account, you need to switch to a personal account to make your profile private **>** Turn off **Suggest your account to others**

19.16.3 Turning Off Suggesting Your Account

By default, TikTok will share your content by featuring it on the **For You** pages of people you do not know.

- If you want to prevent strangers from seeing your videos, you can turn off the **Suggest Your Account** choice.
- Turning this setting off will stop your account being recommended to other users and prevent other people from finding the account via search engines.

19.16.4 Making Videos Private

TikTok allows you configure previously posted or latest videos with specific privacy settings. Videos previously posted can be configured as follows:

- Open a **video**.
- Tap the three-dot icon at the bottom right.
- Select **Privacy** settings.
- Tap **Who can view this video**
- Select **Friends** or **Private.**

Newer videos can be configured as follows:

- Before uploading, tap **Who can view this video**
- Select **Friends** or **Private.**

19.16.5 Managing Duet Control

You can control who can duet on your videos which can be configured as follows:

- Go to the **Privacy and safety** settings choice under the app settings.
- Tap **who can duet with your videos**.
- Choose **Friends or No one** to limit those who can duet with you or your child.
- You can do this for several different options such as who can send you direct messages and download your videos.

19.16.6 Blocking Interactions

TikTok users can interact with your account and content in multiple ways: they can view or download it, direct message you, and duet with your videos.

- The default setting for these interactions is **On**, but you have the choice to change it to **Friends** or **Off**.
- To limit how other users can interact with your videos go to the Safety section of the Privacy page.
- Blocking interactions stops comments, duets, and reactions, and prevents people from seeing your messages or the videos you have liked.

19.16.7 Reporting A User

To block and/or report a user on TikTok you can do so through the following steps:

- Go to the user's profile and tap the three dots at the top of the screen.
- From the options select **Block** or **Report**.
- If you block the user, it will ask you to **confirm** this.
- If you wish to simply report the user, you need to select why you are reporting them.

19.16.8 Enable Two-Factor Authentication

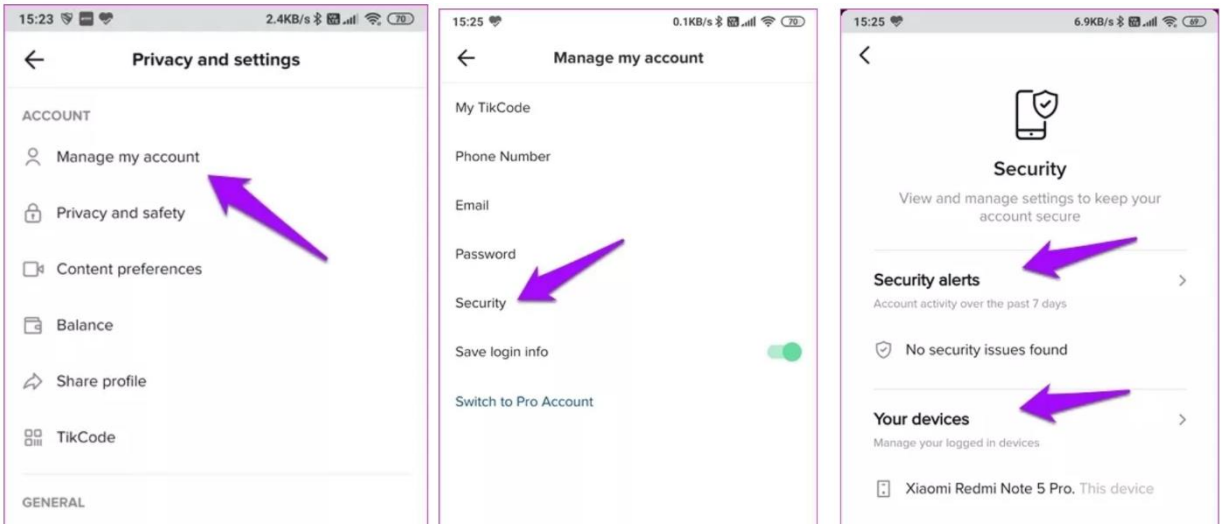
It is always worth enabling 2-factor authentication to add a layer of extra security on you and your child's account. **The verification code can be sent to either your mobile phone or email address**.[380]

- Select **Security** in the settings and privacy menu.
- Tap on **2-step verification**.
- Select your chosen verification method **Phone** or **Email**.

19.16.9 Hacking Attempts And Security Alerts

TikTok has a built-in feature to aid in detecting hacking attempts and suspicious activity on your account.

- By accessing your security alerts, shown below, you can see what devices have accessed your accounts or are trying to access your account without you, you can see what devices have accessed your accounts or are trying to access your account without your permission.

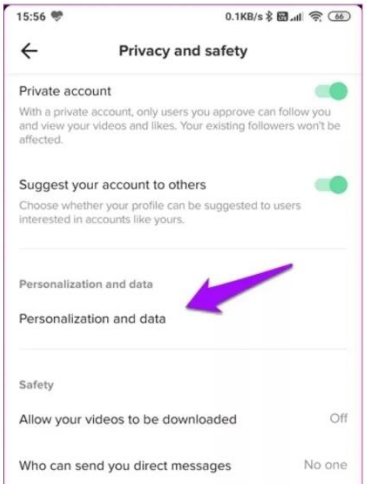


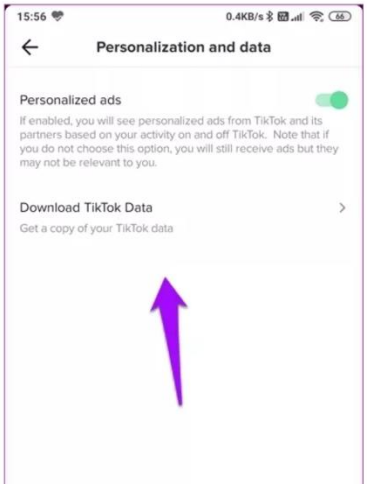
19.16.10 How To Download TikTok Data

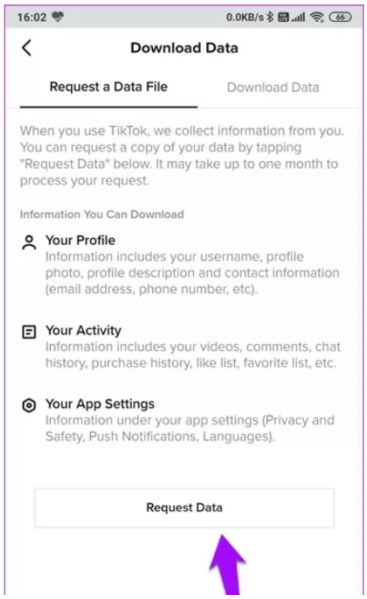
Just like other social media platforms, TikTok also allows you to download your data.

- The option is available under **Personalization and data** under **Privacy and safety**.[381]
- Tap on **Download TikTok Data**, and under the **Request a Data File** tab, tap on the Request Data button to start the process.
- You will receive a confirmation email, followed by the actual file which is usually sent within four days.

- The file will also be available under the **Download Data** tab. This file can be large, depending on how many videos have you uploaded, but that is not the only thing it will have.
- Your contact details and user activity, which includes comments and likes, are also included.







19.16.11 Digital Wellbeing Section: Child Safety

19.16.11.1 Child Safety Settings

Restricted Mode stops most inappropriate content from appearing for children.

- It is also possible to set a passcode to prevent your child from changing this setting later. This setting is also found in the **Digital Wellbeing** section.

19.16.11.2 Family Safety Mode

This setting allows you to assign an account as **Parent** and **Teen**. This gives you remote access over an adolescent's TikTok account.

- Once connected to the account, you can control: Screen Time Management, set how long your child can spend on TikTok each day.

19.16.11.3 Direct Messages

This feature allows you to control who can message your child or turn off direct messages completely.

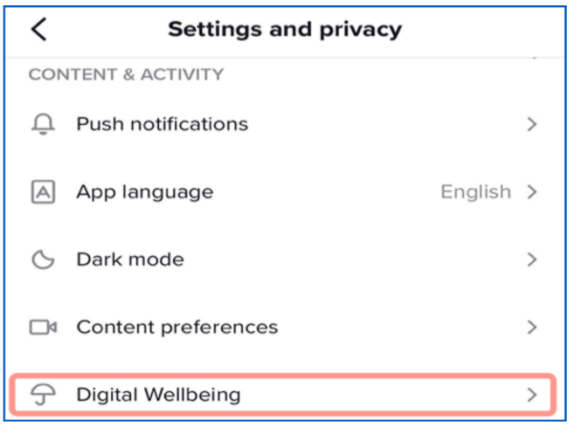
19.16.11.4 Restricted Mode

This feature allows users to restrict types of content that you think are inappropriate for your child.

- It is possible to manage all this from a remote device, so you can make sure your child is always protected.
- This setting is also found in the **Digital Wellbeing** section.

19.16.11.5 Manage Screen Time

If you wish to limit time on the app, go to the **Digital Wellbeing** section of the **Settings & Privacy** page and use the Screen Time Management option to select your time limit.



19.17 TWITTER

Twitter is an online news and social networking site where people communicate in short messages called tweets.[382] Twitter allows users to communicate and stay connected through the exchange of quick, frequent messages.[383]

People post Tweets, which may hold photos, videos, links, and text.[384] These messages are posted to your profile, sent to your followers, and are searchable on Twitter search.[385]

Twitter has extensive information on how to protect your account at the following **URL**.[386]

- You can also find additional information on how to check safety and security settings as well as **How to protect your personal information**. [387]

19.17.1 Sharing Your Personal Information

When someone else Tweets your personal information such as in a doxing attack, you have the right to report the individual to Twitter.[388]

- However, if it is discovered that your personal information is publicly available, Twitter may not request that your information be removed.[389]
- Twitter also provides a link to assess ways to **protect your personal information**.[390]

19.17.2 Your Profile

- In the Twitter menu, click **Profile**.
- Below your header photo, click **Edit profile**.
- This section will allow you to edit your **Bio**, **Location**, and **Website**. It should be noted that this information **will be displayed publicly** unless you adjust the privacy settings.[391]
- Next to **Birth date**, you have the option to click **Edit**. Doing so will allow you to click **Remove birth date** to completely remove it from your profile.
- If you choose to display your birthday, you also have the choice to set the visibility for **Month and day** to something other than **Public** but leave the year as **Only you**.

19.17.3 Public Tweets Versus Protected Tweets

When you sign up for Twitter, your Tweets are public by default meaning anyone can view and interact with your Tweets.[392]

- Should you choose to protect your Tweets, you can do so through your **account settings**.[393]
- Twitter provides extensive detail on how to configure settings for protecting your Tweets. If you protect your Tweets, you will receive a request when new people want to follow you, which you can approve or deny.
- Accounts that began following you before you protected your Tweets will still be able to view and interact with your protected Tweets unless you block them.
- Protected Tweets will not appear in third-party search engines and are only searchable on Twitter by you and your followers.

19.17.4 Photo Tagging

Even if your Tweets are protected, you can be tagged or mentioned in a photo.

- Likewise, your followers may re-share links to photos that you share in a protected Tweet.
- Links to photos shared on Twitter are not protected.
- Anyone with the link will be able to view the content.
- You can change who can tag you in a photo by visiting your Privacy and safety settings via twitter.com and Twitter for iOS or Twitter for Android apps.

19.17.5 Discoverability

Anyone with your email address or phone number can search for you on Twitter using this information.[394]

- Also, anyone with this information in their contacts are provided your account (as a suggestion to follow) once they join Twitter.
- To turn this choice off, go to your privacy settings. Under Discoverability, uncheck **Let others find you by your email** and/or **Let others find you by your phone**.

19.17.6 Sharing Your Location In Tweets

Tweet location is off by default. You would need to opt in for this service.

- Once activated, Twitter will supply suggestions for locations of your next Tweet, but you can still choose not to share your location for individual Tweets.
- If you choose to enable precise location through Twitter's official apps, **this will allow Twitter to collect, store, and use your precise location**, such as GPS information.[395]

19.17.7 Third-Party Businesses And Personalized Ads

Even if you have turned off personalized ads and sharing data with third party businesses in your settings, Twitter shares information with business partners to help improve its business and ads will be shown based on your Twitter activity, information you have provided, as well as the devices you have used to log in.[396]

- Turning off these options simply reduces the relevance of the marketing activities on other sites, apps, and advertisements to you.

19.17.8 Blocking An Account

Blocked accounts cannot follow you, send direct messages to you, or tag you in a photo.

- They can view your public Tweets if not logged into Twitter.
- Blocked accounts do not receive a notification alerting them that their account has been blocked.
- However, if a blocked account visits the profile of an account that has blocked them, they will see they have been blocked, unlike **mute** which is invisible to muted accounts.[397]

19.17.9 Two-Factor Authentication

Twitter offers two-factor authentication but instead of only entering a password to log in, you will also enter a code or use a security key.[398]

- This added step helps make sure that you, and only you, can access your Twitter account.
- During enrollment, Twitter will also verify that you have a confirmed email address associated with your account.
- After you enable this feature, Twitter will require your password, along with a secondary login method — either a code, a login confirmation via an app, or a physical security key to log in to your account.[399]

19.17.9.1 Account Access

- This feature allows you to **review the apps and devices connected to your Twitter account**.[400]
- If there are any that do not truly need access to your Twitter account, click them, then click **Revoke access**.

- You can also access the **Sessions** section to review if there are any devices that do not truly need access to your Twitter account, click them, then click **Log out the device shown**.

19.18 YOUTUBE

YouTube is a video sharing service where users can watch, like, share, comment and upload their own videos. The video service can be accessed on PCs, laptops, tablets and via mobile phones. Users of YouTube can search for and watch videos, create a personal YouTube channel, upload videos to their channel as well as like, comment or share other YouTube videos.[401]

19.18.1 YouTube Subscription Privacy Settings

- You can choose to make which channels you are subscribed to private or public.[402] By default, all settings are set to private.[403]

19.18.1.1 Public Listings

When your subscriptions are set to public, other users can see what channels you subscribe to.

- Your subscriptions are listed on your channel homepage. Your account is listed in the Subscribers List for any channel you subscribe to.

19.18.1.2 Private Listings

When your subscriptions are set to private, no other users can see what channels you subscribe to. Your account does not show in a channel's Subscribers List, even if you are subscribed.[404]

- If you take part in a subscriber-only live chat, other viewers will publicly see you are subscribed to the channel.

19.18.2 Privacy Channel Subscriptions

- Sign into **YouTube**.
- In the top right, click your **profile picture** .
- Click **Settings** .
- In the left Menu, select **Privacy**.
- Turn on or off **Keep all my subscriptions private**.

19.18.3 Hide Subscriber Count

By hiding your subscriber count, it will not be publicly visible to others on YouTube. You can still see your subscriber count from YouTube Studio.

- Sign into your **Google Account**.
- Go to **YouTube Studio**.
- Click **Settings > Channel > Advanced settings**.
- Under **Subscriber count**, uncheck **Display the number of people subscribed to my channel.**
- Click **Save**.

19.18.4 Location-based Recommendations

When you start using YouTube Music, location-based recommendations are turned off. Location helps YouTube Music offer you personalized music recommendations based on where you are. You can change your location-based settings to turn them on or off. Location history is automatically turned off for made for kid's content.[405]

- Visit **music.youtube.com**.
- Select your **profile picture** .
- Select **Settings** .
- Select **Privacy**.
- Make sure **location-based recommendations** are paused. This setting will prevent you from getting location-based recommendations.

19.18.5 Disable YouTube Ads

YouTube uses your data to improve your experience, like reminding you what you have watched, and giving you more relevant recommendations and search results.

- Your activity and information can also be used to personalize ads within YouTube and other Google Services. You can manage activity data in **Your Data in YouTube**.
- The ads that play on YouTube videos you watch are tailored to your interests. They are based on your Google Ad Settings, the videos you have watched, and whether you are signed in or not.
- You can control the ads that you see based on your Google Account **Ad Settings**.
- You can also **view, delete, or pause your YouTube watch history**.[406]

19.18.6 Supervised Kids Accounts On YouTube

Before you can begin setting up the supervised account for YouTube, you will need to have created your child's Google account through **Family Link**.[407]

- **Supervised YouTube accounts are available for kids under 13**, but that age may differ depending on what **country you live in**.[408]

Once this is done, you can begin setting up the supervised account for your child to explore YouTube. To do so, the following steps will walk you through that process.

- Open the **YouTube app** on your phone.
- Tap on your ****profile picture**** in the upper right corner of the screen.
- Choose **Settings** at the bottom of the screen.
- Select **Parent Settings** towards the top of the page.
- If you have multiple child accounts created in Family Link, **choose the account you want to set up** for a supervised YouTube Account.
- Tap on **Set up YouTube**.
- Choose **SELECT** after **reviewing the information** about the type of content that may be available to your child.
- Pick the ****content settings**** for your child's age.
- Scroll through the **Parent feature tour**, then tap **NEXT**.
- Read the information **YouTube's privacy policies** and choose **FINISH SETUP**.

19.18.7 YouTube Kids Parental/Guardian Permission

You must be at least 13 years old to access YouTube Kids (*where available*) if enabled by a parent or legal guardian.[409]

- If you are under 18, you represent that you have your parent or guardian's permission to use the Service.
- It is recommended that your child read this agreement with you.
- You can find tools and resources to help you manage your family's experience on YouTube (***including how to enable a child under the age of 13 to use the Service and YouTube Kids***) in the **Help Center and through** Google's **Family Link**.[410]

20 GOOGLE TRACKING AND LOCATION DATA

Google is an internet search engine. It uses a proprietary algorithm that is designed to retrieve and order search results to supply the most relevant and dependable sources of data possible.[411]

Settings are available to control Google's vast ability to collect data about you in its Activity Controls for your Google account.[412, 413, 414, 415] The easiest way to begin accessing the extensive controls that Google offers users is through the Google Safety Center found at the following **URL**. [416]

20.1 GOOGLE ACCOUNT PRIVACY CONTROLS

Browser Privacy Control	URL
Google Safety Center	https://safety.google/privacy/privacy-controls/
Google Account Privacy Checkup	https://myaccount.google.com/privacycheckup
Google Account Activity Controls	https://myaccount.google.com/activitycontrols
Google Dashboard (Manage All Of Your Google Data)	https://myaccount.google.com/dashboard
Control Web and App Activity	https://support.google.com/websearch/answer/54068?p=web_app_activity&authuser=0&hl=en&visit_id=637056287600533942-3442343815&rd=1
Manage Your Location History	https://support.google.com/websearch/answer/3118687?visit_id=637056287600533942-3442343815&p=location_history&hl=en&rd=1
Auto-Delete Web and App Activity	https://myactivity.google.com/myactivity?restrict=waa
Manage YouTube Privacy Settings	https://support.google.com/youtube/topic/9257518?hl=en
Your Google Data In Search	https://myactivity.google.com/privacyadvisor/search
Your Google Data In Maps	https://myaccount.google.com/yourdata/maps
Your Google Data In The Assistant	https://myaccount.google.com/yourdata/assistant
Download Your Google Account Data	https://takeout.google.com/settings/takeout?pli=1
Google Ad Settings	https://adsettings.google.com/authenticated?utm_source=udc&utm_medium=r
Google Maps Timeline	https://support.google.com/maps/answer/6258979
Search Activity	https://support.google.com/websearch/answer/54068?co=GENIE.Platform%3DDesktop&hl=en
Shared Usage and Diagnostic Data	https://support.google.com/accounts/answer/6078260
Google Security Tips	https://safety.google/security/security-tips/
Google Security Tips-Parental Supervision	https://safety.google/families/parental-supervision/
Google Security-Tips For Families	https://safety.google/families/families-tips

20.2 Google Assistant Data Privacy Controls

In 2019, Google outlined substantial changes to how Google Assistant handles voice recordings.[417] These changes originated to meet users' expectations of data transparency.[418]

- If you use Google Assistant, the table below has the URL you can use to browse or delete your Google Assistant data to include your Web and App activity, Voice and Audio recordings, App and Contact information from your devices and Ad personalization.

Browser Privacy Control	URL
Google Assistant	https://myaccount.google.com/yourdata/assistant?e=PrivacyAdvisorAssistant&pli=1

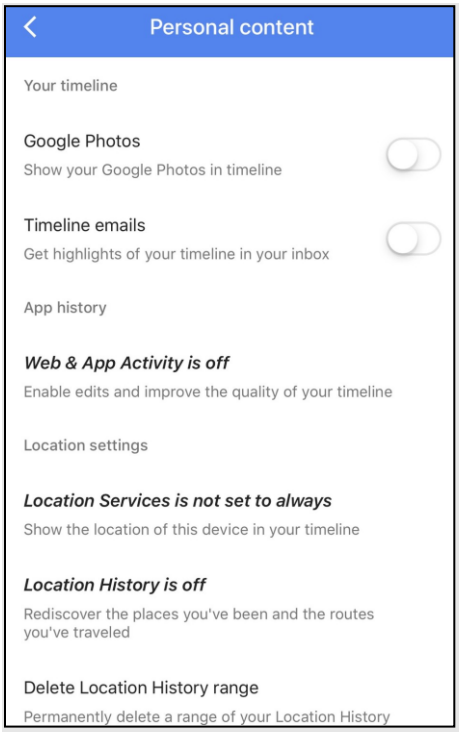
20.3 Calendar Privacy Controls

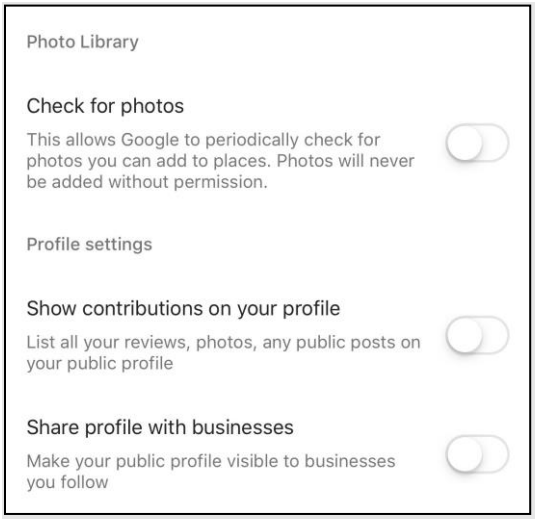
Gmail users are vulnerable to malicious or unsolicited Google Calendar notifications. Google Calendar allows anyone to schedule a meeting with you, and Gmail is built to integrate with this calendaring functionality.[419]

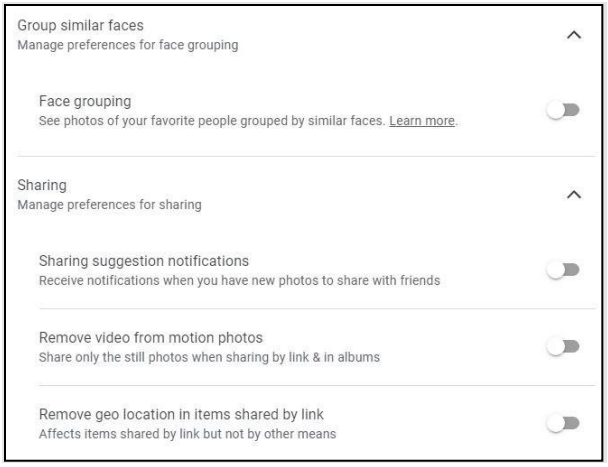
- When a calendar invitation is sent to a user, a pop-up notification appears on their smartphone.
- Threat actors can create messages to include a malicious link, which can be used in phishing schemes or social engineering attacks.[420]

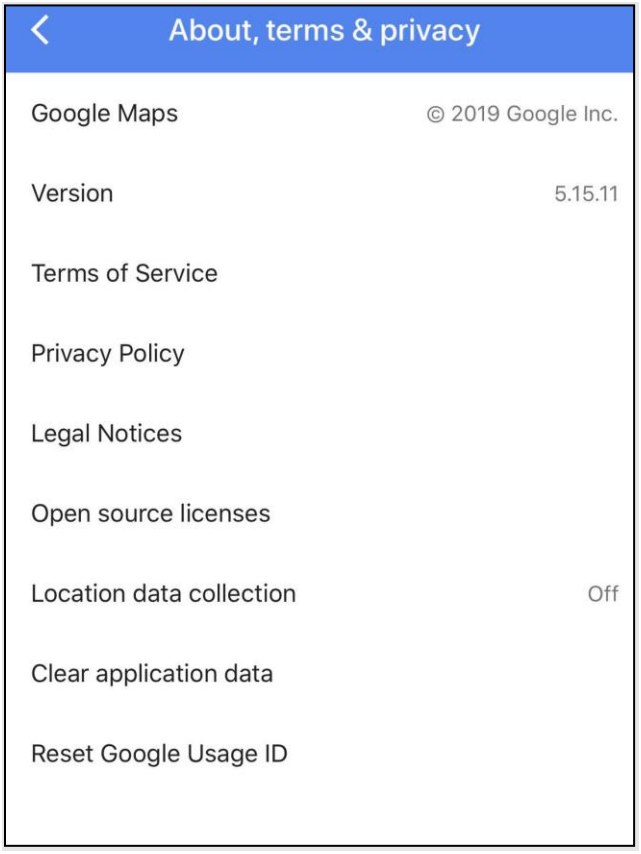
Browser Privacy Control	URL
Google Calendar	1. https://support.google.com/calendar/answer/37083?hl=en
	2. https://support.google.com/calendar/answer/37082?hl=en&ref_topic=3417970
Google Events	1. https://support.google.com/calendar/answer/6084018?co=GENIE.Platform%3DDesktop&hl=en

20.4 PRIVACY IN PERSONAL CONTENT






Group similar faces
Manage preferences for face grouping
Face grouping
See photos of your favorite people grouped by similar faces. Learn more.
Sharing
Manage preferences for sharing
Sharing suggestion notifications
Receive notifications when you have new photos to share with friends
Remove video from motion photos
Share only the still photos when sharing by link & in albums
Remove geo location in items shared by link
Affects items shared by link but not by other means


About, terms & privacy
Google Maps
© 2019 Google Inc.
Version
5.15.11
Terms of Service
Privacy Policy
Legal Notices
Open source licenses
Location data collection
Off
Clear application data
Reset Google Usage ID

21 AMAZON

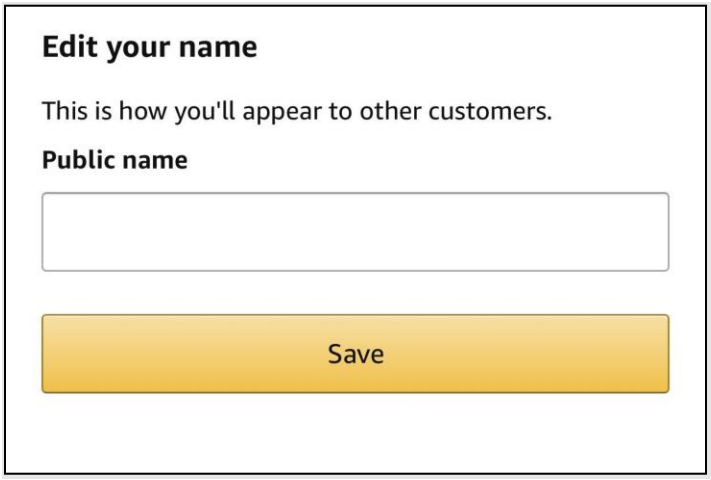
Amazon is a cloud computing giant and the largest American e-commerce company.[421] Amazon collects your personal information with what you provide them[422] and will use your personal information to communicate with you about your purchases of products and services, improve and personalize your Amazon experience, and follow legal obligations, among others.[423]

- In addition, Amazon uses your personal information to display interest-based ads[424] for features, products, and services that might interest you and cookies and other identifiers to enable recognition of your browser or device.[425]

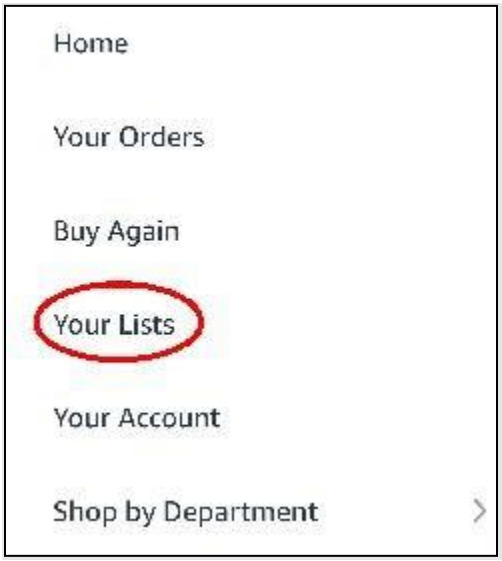
21.1 AMAZON PRIVACY SETTINGS

Visit the following **URL** to learn about default Amazon settings to improve your privacy. Follow steps below to act at once.[426]

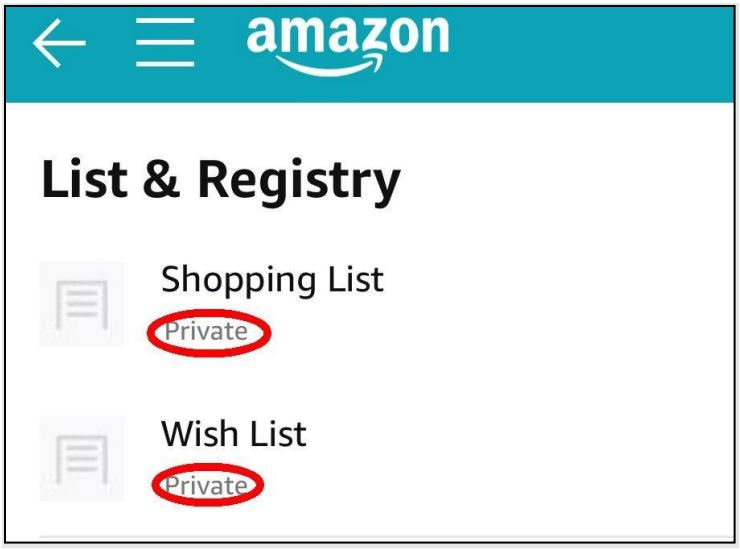
21.1.1 Removing Your Public Profile



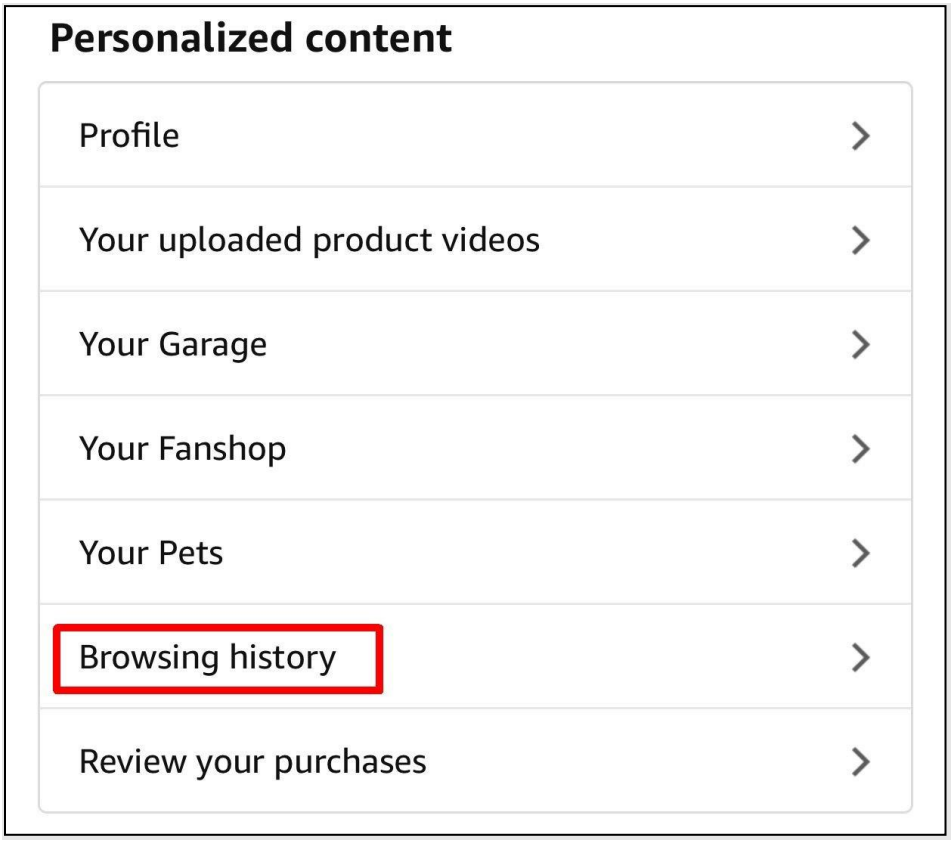
21.1.2 Private Shopping And Wish Lists



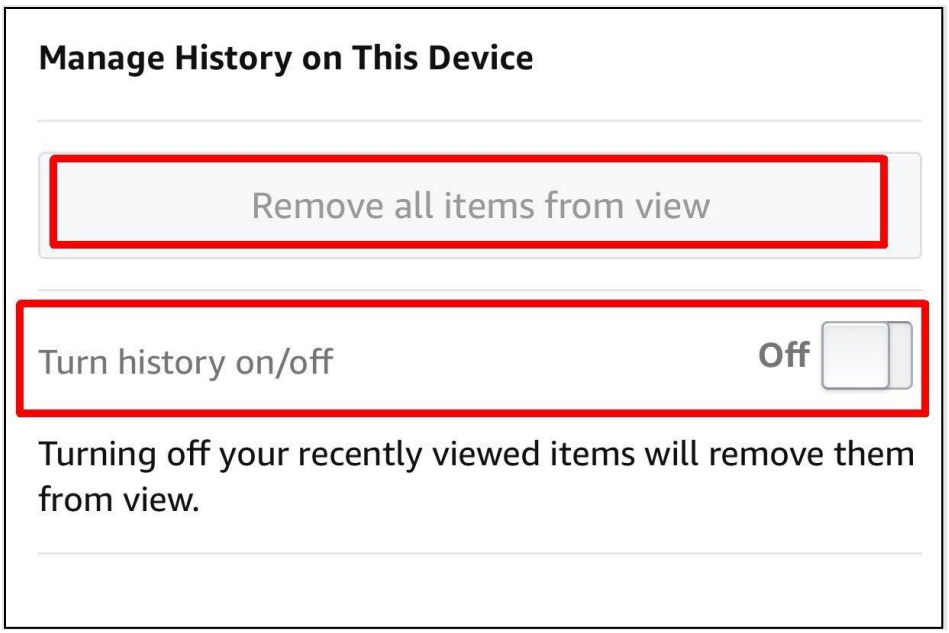
Then,



21.1.3 Browsing History And Tracking Cookies

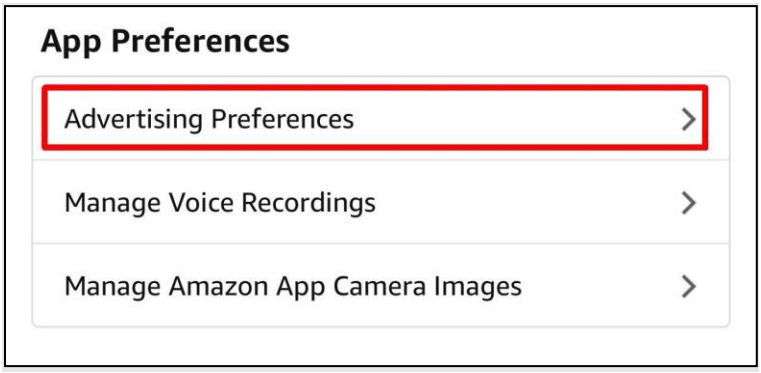


Then,

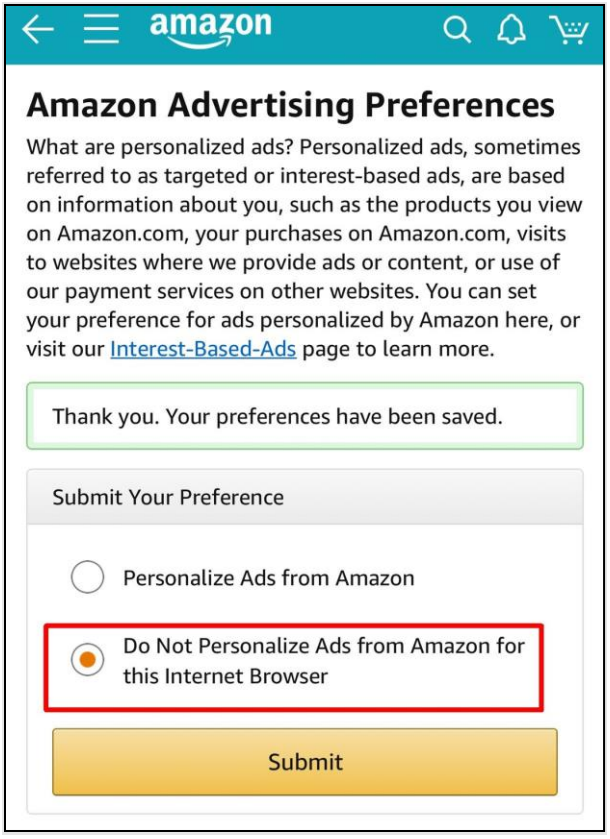


21.1.4 Opting Out Of Advertising Preferences

Skip this section if you would like Amazon's ability to track your activities and to market items to you.

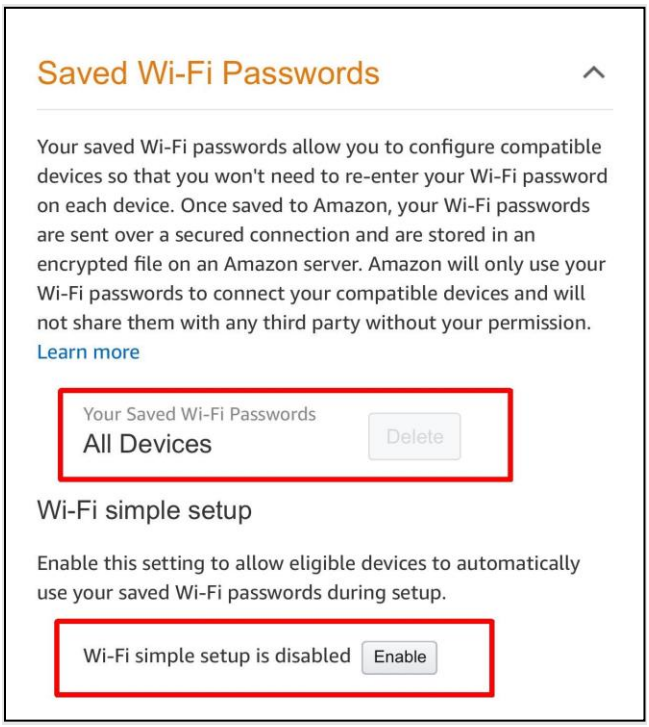


Then,



21.1.5 Disabling Amazon Saved Wi-Fi Passwords

Ever wonder why you did not have to put your Wi-Fi password into your Fire TV or Alexa Echo? It is because this setting is enabled.[427]



21.1.6 Deleting Wi-Fi Passwords From Amazon

To delete Wi-Fi passwords saved to Amazon using your web browser[428]:

- Go to **Manage Your Content and Devices** > **Preferences** > **Saved Wi-Fi Passwords** > **Delete**

21.1.7 Deleting Wi-Fi Passwords From Kindle

To delete Wi-Fi passwords saved to Amazon from your compatible Kindle e-reader[429]:

- **Home > Settings > All Settings > Wi-Fi and Bluetooth > Delete Saved Wi-Fi Passwords > Delete** to confirm.

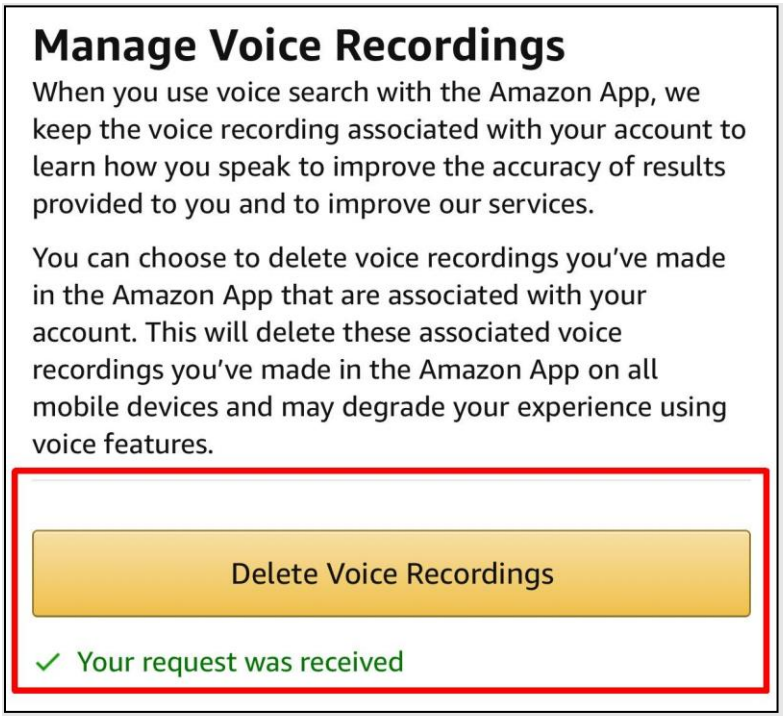
21.1.8 Deleting Wi-Fi Passwords From Fire TV

To delete Wi-Fi passwords saved to Amazon from your compatible Fire TV device[430]:

- **Settings > Network > Save Wi-Fi Passwords to Amazon**.
- Press the **Select** button on your remote to turn off saved Wi-Fi passwords, and delete passwords saved to Amazon.

It should be noted that deleting Wi-Fi passwords from your Fire TV will only delete passwords saved to Amazon from that device.

21.1.9 Disabling Voice Recordings



21.1.10 Disabling Camera Images

Then,

21.2 Amazon Security Settings

21.2.1 Security Alerts

If you get a Security Alert about activity you do not recognize, click or tap the **Not Me** option in the notification so we can help you **reset your Amazon password** immediately to secure your account.[431]

- If you are not able to sign into Amazon because you do not have access to the email or mobile phone on your account anymore, contact Customer Service for help restoring access.[432]

21.2.2 Two-Step Verification

It is highly recommended you enable this feature in Amazon.

- When you try to log in, Two-Step Verification sends you a unique security code.

- Per Amazon, when you sign up for **Two-Step Verification**, Amazon will **send you a unique code by text message, voice call, or authenticator app**.[433] [434]
- The following **URL** takes the mystery out of enrolling in this feature.[435]

21.2.3 One-Time Passwords For All Devices

After enrolling in Two-Step Verification, it is recommended a user not suppress any future One-Time Password (OTP) challenges as this moves you from the realm of Two-Factor Authentication to a **Multi-Factor Authentication** posture within Amazon.[436]

- This feature allows you to enable a requirement for OTP on all devices. It is recommended users enable this feature.

21.2.4 Secure Delivery with One-Time Password

If you want to take your Operational Security to the next level it is recommend users enable **Amazon's One-time password (OTP) verification feature**.[437]

- By enabling OTP verification, Amazon will send you a six-digit numeric PIN code that is valid until the end of the day adding yet another layer of security to your packages.
- Should you be delayed and miss the designated rendezvous point and time of package delivery, Amazon has you covered in case as they will re-attempt delivery the next day or if you have a trusted contact, you may share the OTP with whoever you choose to receive the package on your behalf.
- Remember to never share the OTP with the delivery agent over phone as OTP is intended for you to ensure secured delivery of the package.

21.2.5 1-Click Settings

1-Click lets you associate a credit, debit, or Amazon Store Card with addresses you ship to often so you can place orders with a single click of a button.[438]

- When you disable **1-Click it only disables 1-Click for orders that can be shipped.** 1-Click ordering does not affect digital purchases.[439]
- Since your browser must be cookie-enabled to use 1-Click shopping, if your browser is not cookie-enabled, you can still buy items by adding them to your Shopping Cart and clicking **Proceed to checkout.**
- It is recommended using the **Disable 1-Click everywhere** setting which you can also enable for your Mobile orders at the following **URL** to ensure you do not fall victim to a scam.[440]

21.3 Amazon Alexa Echo Settings

21.3.1 Review Your Alexa Voice History

You can review, listen to, or delete your voice recording history from the Alexa app or Your Account.

- **Alexa app > More > Settings > Alexa Privacy > Review Voice History** and then select an entry, review a specific date range, or filter by device or voice ID.

Amazon states that voice recordings are used to improve the accuracy of your interactions with Alexa, deleting voice recordings does not delete your Alexa Messages and voice recordings are visible until the deletion request has finished processing.[441]

21.3.2 Ask Alexa to Delete Your Voice History

To ask Alexa to delete your voice recordings, enable deletion by voice in the Alexa app.[442]

- **Alexa app > More > Settings > Alexa Privacy > Manage Your Alexa Data >** turn **Enable deletion by voice On or Off**

Then you can use your voice to delete your voice recordings for the period you want.

- Say, "Delete what I just said."
- Say, "Delete everything I said today."
- Say, "Delete my entire voice history."

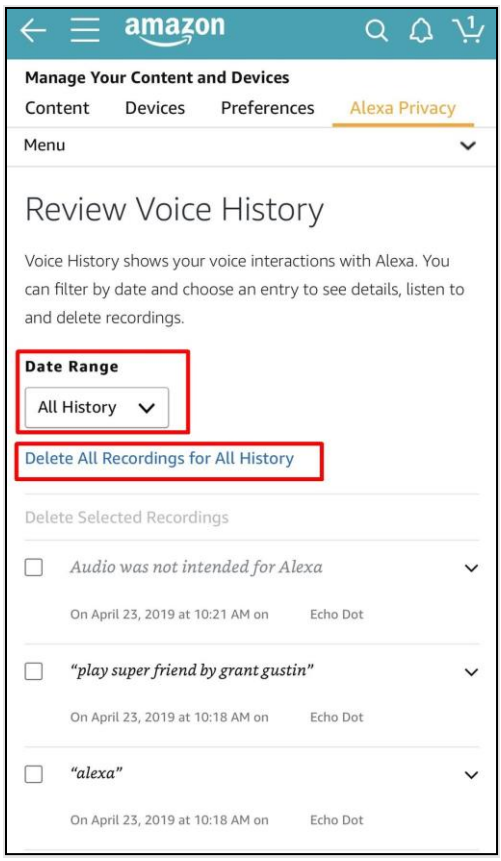
Amazon states that voice deletion is not supported on FreeTime-enabled Alexa devices[443]. To manage voice recordings from a FreeTime-enabled Alexa device, ask another Alexa-enabled device on the account or use the Alexa app.[444]

21.3.3 Delete Alexa Voice Recordings

You can set your account to automatically delete Alexa voice recordings as this feature is disabled by default.[445]

- **Alexa app > More > Settings > Alexa Privacy > Manage Your Alexa Data > Automatically delete recordings > Off**
- Choose a period to keep your voice recordings and then select **Confirm**.

Amazon states that when choosing **Don't save recordings**, it may take up to 36 hours for our systems to apply this setting. Voice recordings older than the selected period are deleted automatically.



21.3.4 Disable Voice Purchasing On Alexa

You can limit buying so that only recognized household members can place orders with Alexa.[446]

- Open the Alexa app .
- Open More and select Settings.
- Select Account Settings.
- Select Voice Purchasing.
- Turn Voice Purchasing on or off.

21.3.5 Manage An Alexa Voice ID For Purchases

You can use the Alexa app to turn on or turn off an Alexa voice ID to place orders with Alexa. Managing an Alexa voice ID ensures that only recognized household members place orders with Alexa.[447]

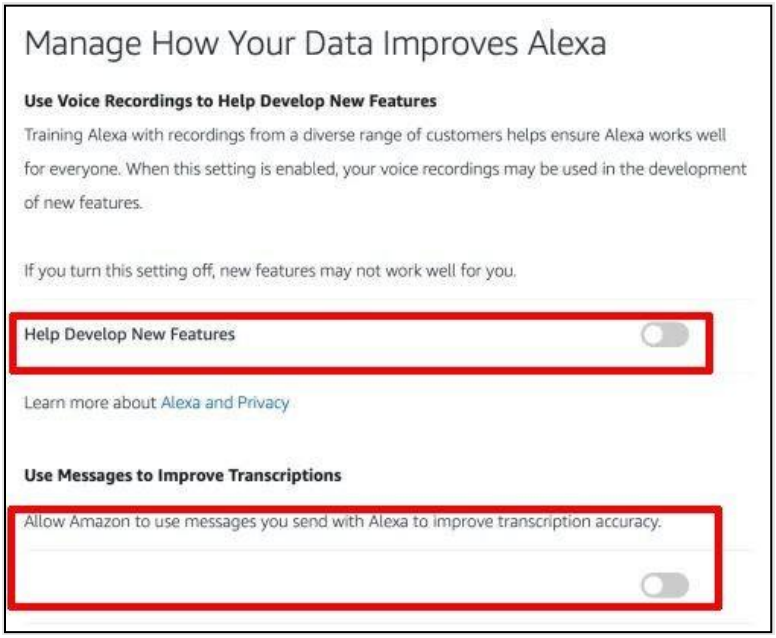
- **Alexa App > More > Settings > Account Settings > Voice Purchasing > Purchase Controls > Only Recognized Voices >** Select who can make voice purchases

21.3.6 Require a Voice Code For Purchases

Users can set a 4-digit voice code to confirm purchases or prevent accidental orders.[448]

- **Alexa App > More > Settings > Account Settings > Voice Purchasing > Purchase Confirmation > Manage >** Turn **Voice Code** on and set your 4-digit voice code.

21.3.7 Managing Your Data Improving Alexa



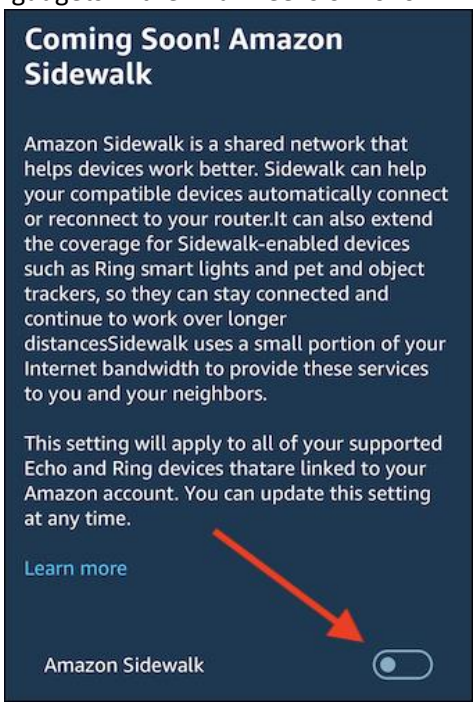
21.3.8 Disabling Motion Detection

Amazon outlines that **ultrasound motion detection** is available on **Echo Dot (4th Generation)** devices and **Echo (4th Generation)** devices. The devices do not emit ultrasound until you turn on a feature that uses motion detection, such as **Occupancy Routines** as humans cannot hear or perceive ultrasound.[449]

- **Alexa App > Devices > Echo & Alexa > Device Echo > Settings** via gear **> Motion Detection > Toggle** to turn the feature on or off as you choose.

21.4 Amazon Sidewalk Opt Out

Amazon Sidewalk is a new feature rolling out to Amazon-branded gadgets in the final weeks of 2020.[450] This service is designed to act as a backup network in the event Ring and Echo devices lose their internet connection.[451]



- Amazon Sidewalk allows select Echo and Ring devices to piggyback off nearby Amazon gadgets' connections.[452]
- This can include devices belonging to other people in other houses.[453]
- If a user has Amazon Sidewalk enabled on their Ring or Echo, their devices can use your connections in an outage as well.[454]
- If you have not done so already, it is highly recommended users read the Amazon Sidewalk Privacy and Security Whitepaper.[455]

21.4.1 Disabling From The Alexa App

- **Alexa App** **> More** **> Settings > Account Settings > Amazon Sidewalk**.
- Turn Amazon Sidewalk **on** or **off** for your account.

If you do not have a mobile phone with the Alexa app, you can change this setting from the web. Select Enabled or Disabled under Amazon Sidewalk in **Manage Your Content and Devices > Preferences**. It should be noted that the Sidewalk setting only appears when you have a compatible Echo device linked to your Amazon account. The website version of the Alexa app does not show this setting. When you turn Amazon Sidewalk on or off, the same setting will be applied to all your devices.[456]

22 GAMING CONSOLES

Gaming consoles like the Nintendo Switch, PlayStation 4, and X-Box One all have social media services. Check the below settings and advice for controlling your accounts' privacy.[457]

22.1 CONSOLES AND ONLINE SERVICES

Service	Privacy Settings/Advice
Nintendo Switch	https://en-americas-support.nintendo.com/app/answers/detail/a_id/15987/~/how-to-adjust-nintendo-account-profile-settings-%28country%2C-email%2C-etc.%29
PlayStation 4 (PS4) and PlayStation Network (PSN)	https://www.playstation.com/en-gb/get-help/help-library/my-account/parental-controls/how-to-use-playstation-4-to-limit-who-can-contact-you-over-plays/ https://www.playstation.com/en-us/account-security/2-step-verification/ https://thenextweb.com/basics/2019/01/31/playstation-4-privacy-settings-hiding/
X-Box One (XONE) and X-Box Live	https://support.microsoft.com/en-us/help/4482922/xbox-one-online-safety-and-privacy-settings-for-parents-and-kids https://www.thewindowsclub.com/how-to-setup-xbox-privacy-and-online-safety-for-kids

23 CONNECTED TV (CTV) AND OVER-THE-TOP (OTT) DEVICES

Connected TV (CTV) and Over-the-top (OTT) devices are two exceedingly popular methods of accessing TV/video content, but they can be easily confused for one another.

A Connected TV (CTV) is a device that connects to—or is embedded in—a television to support video content streaming. Distinct types of CTVs include Xbox, PlayStation, Roku, Amazon Fire TV, Apple TV, and more.

Over-the-top (OTT) is the delivery of TV/video content directly from the internet. Users do not have to subscribe to a traditional cable or satellite provider to access this content; they can watch this content on various devices—tablet, phone, laptop/desktop, television, etc. The video is delivered in a streaming or video-on-demand (VOD) format. Different types of OTT services include Netflix, Hulu, and Amazon Prime. Mass media and networks are also launching their own OTT services such as Disney+ and NBC's Peacock.

The rise of CTV and OTT has led to the phenomenon known as "cord-cutting", which is the growing trend of customers canceling their traditional cable and satellite subscriptions in favor of only using these streaming or VOD formats.[458]

With more than 164 million U.S. users accessing video content via connected TV devices and predicted to grow by up to 204.1 million viewers in 2022, it is no surprise that marketers are looking for ways to use online advertising through CTVs.[459]

It should also be noted the number of Smart TV's and OTT (over-the-top) devices in households exceeded 1 billion in 2019. In the U.S. alone, more than 50% of the population has a TV-connected device in their home.[460]

23.1 ADVERTISING ON CTVS AND OTTS

The growing concern over online data and user privacy has been focused on tech giants, social media platforms and smartphones but people's data is being quietly and increasingly siphoned right out of their living rooms via their televisions, oftentimes without their knowledge.[461]

Many TV streaming devices and smart TVs include unique advertising identifiers and can collect data about the content viewed by users, as well as the user's interaction with some applications available on these devices, for digital advertising purposes.[462] [463] The operating systems on many of these devices include built-in settings to help users express privacy preferences for digital advertising data collection and use, but only a minority of users even know how to use these preferences.

Your CTV or OTT device collects data about what you watch to improve your viewing experience, while also monetizing this data through targeted advertising.[464] Most people do not realize know how much data CTVs and OTT devices collect, how that data is used, and how it impacts their lives beyond the TV screen — a potentially significant IoT security risk.[465] Because many people connect all their smart devices to a single Wi-Fi router, a hacker could access your entire network by hacking one smart appliance or router.[466] If you would like to know more about the many ways that CTVs and OTTs deliver advertising content to the consumer, the following **URL** is incredibly helpful and packed with insight into the process.[467]

23.2 Opting Out Of Advertising On CTVs and OTTs

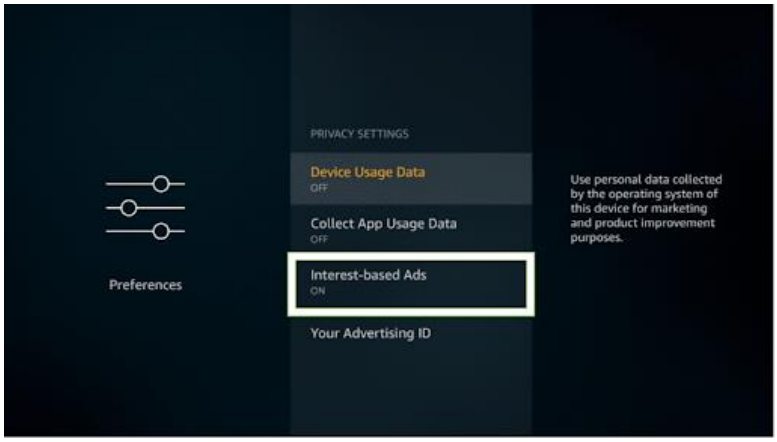
Below are instructions pulled from the **NAI page** which helps users find and change the privacy preferences on many commonly used CTVs and OTTs to limit digital advertising data collection on these devices to the extent that the device's manufacturer will allow.[468]

Some companies may offer added or alternate choices depending on their technology (such as resetting an advertising ID or turning off the associated service). You should always contact the provider of the opt-out mechanism if you experience any issues or have questions about its functionality. By design, it is easy to inadvertently consent to having your data collected and sold to advertisers from Connected TVs and Over-The-Top devices. While most of us have these devices in our homes, only a minority of us know how to deactivate many of these features should we choose.

It should also be noted that most companies will apply privacy preference to digital advertising data collection and use practices for the device on which the preference is expressed, but not for data collection and use on any added devices. Privacy settings for web browsers on CTVs or OTTs are typically independent from the privacy preferences described on this page. To learn more about expressing your privacy preferences in a web browser, please visit the **NAI's opt-out page**.[469]

23.2.1 Amazon Fire TV

Settings -> Preferences -> Privacy Settings -> Interest-based Ads -> Off



23.2.2 Apple TV

Settings -> General -> Privacy -> Limit Ad Tracking -> On

23.2.2.1 Pre-2015 Apple TV

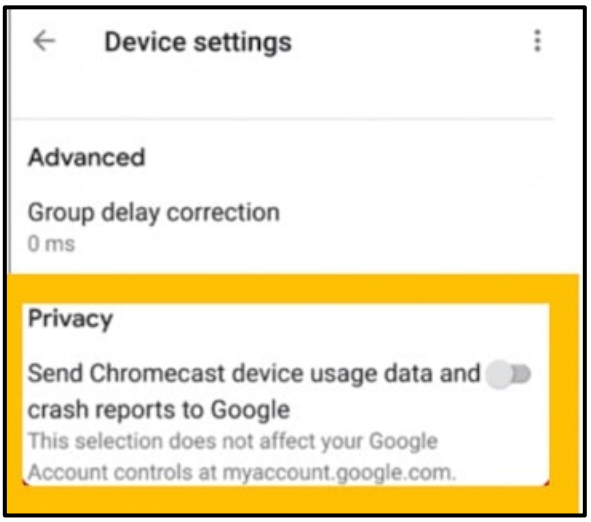
General -> Send Data to Apple -> No

If you are using **Family Sharing** the organizer of the group must allow other members to make modifications:

Settings > General > Restrictions > Advertising > Allow modifications

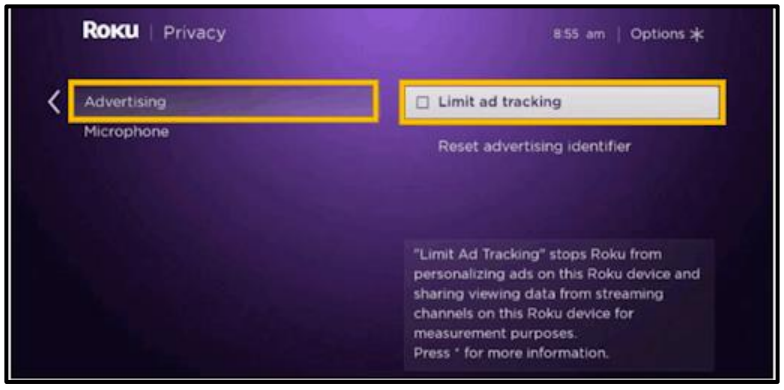
23.2.3 Google Chromecast

Menu > Devices > Device Icon > Press **three dots** in the upper left **corner > Settings > Send Chromecast device usage data and crash reports to Google >** Uncheck the box



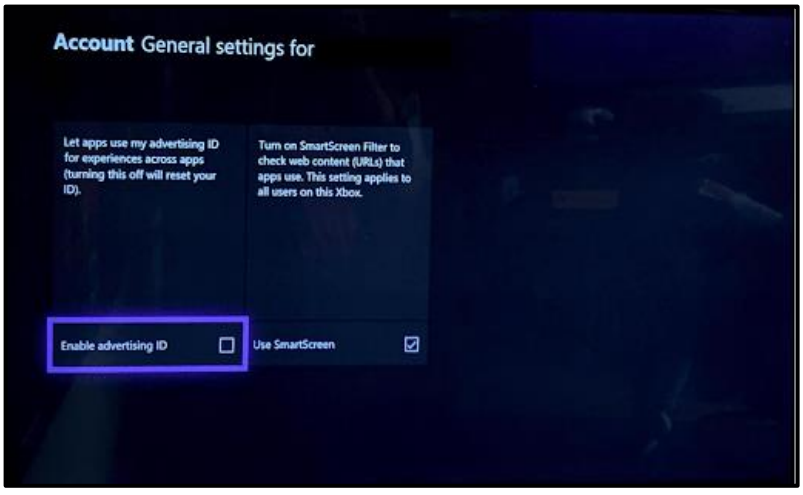
23.2.4 Roku

Settings > Scroll to Privacy > Advertising > Limit Ad Tracking



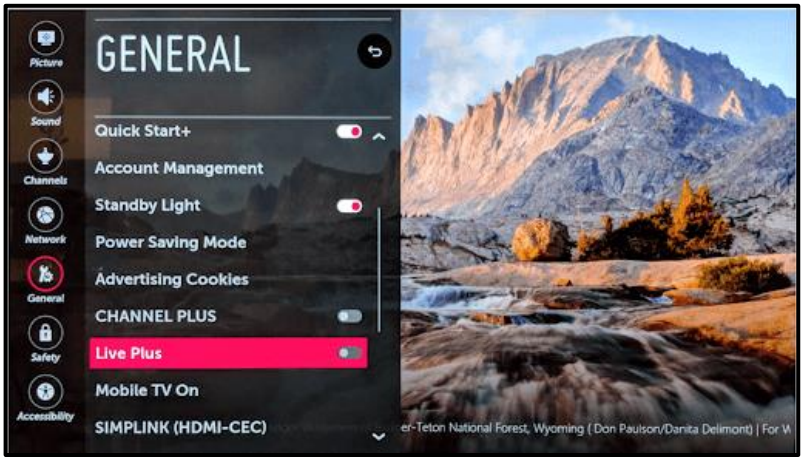
23.2.5 Xbox

System > Settings > Account > Privacy and Online Safety > App Privacy > General > Enable Advertising ID > Uncheck



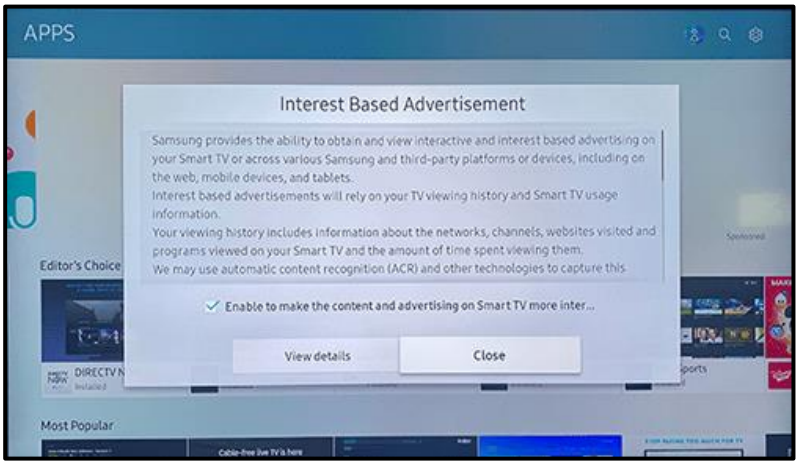
23.2.6 LG TV

Settings > General > LivePlus > Uncheck



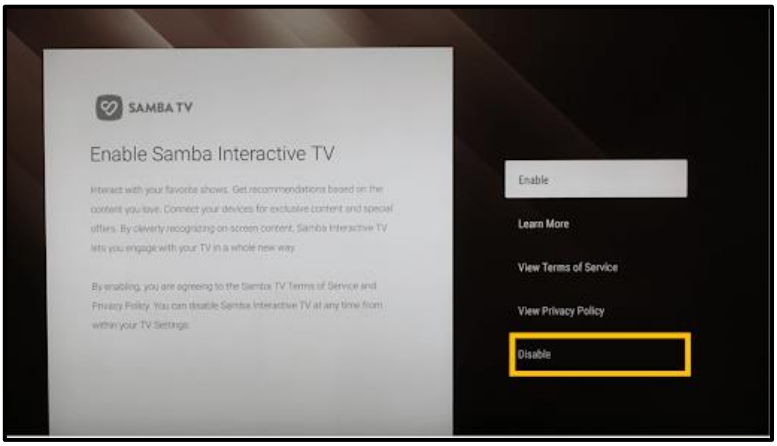
23.2.7 Samsung TV

Settings > Support > Terms & Policies > Internet Based Advertising > Off



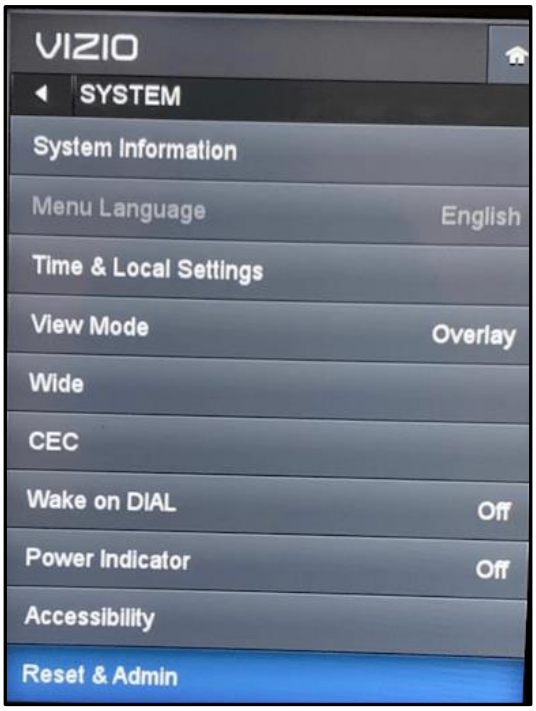
23.2.8 Sony TV

Settings > Network > Samba Interactive TV > Disable/Off



23.2.9 Vizio TV

Menu button on remote or open **HDTV Settings** app **> System > Reset & Admin > Highlight Viewing Data >** Press right arrow to change the setting to **Off**



24 HOME SECURITY CAMERAS

Home security cameras have become extremely popular in recent years for the convenience of seeing who is at your house as well as being a terrific way to protect your home and belongings against a range of threat actors.[470] However, since many of the cameras are connected to the internet, they can present some privacy issues if not configured correctly.[471] Below we discuss features to look for to safeguard your privacy when picking out a security camera and give you a breakdown of some of the best cameras that meet these standards.[472]

24.1 SECURITY CAMERA FEATURES TO CONSIDER

24.1.1 Connectivity

Wireless and wire-free cameras can be vulnerable to hacking and signal drops so consider using cameras that have a wired connection to the internet for the best protection.[473]

24.1.2 Two-Factor Authentication

Enabling Two-factor authentication is a terrific way to add an added layer of protection to your cameras, making the camera not easily comprisable.[474]

24.1.3 Privacy Shutter

Putting privacy shutters in place by one of the following methods can prevent unwanted guests from streaming or recording footage from your camera: putting a physical cover over the camera, enabling it through an app, or pressing a switch on the camera.[475]

24.1.4 Local Storage

As an alternative to storing all your camera's videos on the cloud, you can store the videos locally onto a memory card, microSD, to ensure the safeguarding of your privacy.[476]

24.1.5 Detection Zones

Cameras with detection zones allow you to select the areas in a frame you want to watch which drops the need for continuous recording, as in camera models that record anytime motion is detected and cuts down on the storage needed for your footage.[477]

24.1.6 Facial Recognition

Facial Recognition is a feature available on some camera models that can be programmed to only record when faces that are unknown are present. This means the camera will not actively record and send you alerts unless it is a stranger or someone the feature does not recognize.[478]

24.2 Camera Feature Comparison Scorecard

Below is a table that serves as a scorecard for some of the top security cameras when it comes to the features discussed above to aid in privacy.[479]

Camera	Two Factor	Privacy Shutter	Local Storage	Detection Zones	Facial Recognition
Wyze Cam V3	X		X	X	
Google Nest Cam IQ Indoor	X	X		X	X
CYNC Indoor Cam	X	X	X	X	
Eufy Security Indoor Cam 2K Pan and Tilt		X	X	X	X
D-Link DCS8300 Wi-Fi Camera	X		X	X	
Simplisafe Simplicam	X	X		X	
Arlo Essential Indoor Security Cam	X	X		X	
Logitech Circle View	X	X		X	X

24.3 Tips for Keeping Your Camera Safe

After you have bought the camera there are some added steps you can take to ensure your camera stays safe once it is in your home.[480]

- Choose a router with security that will encrypt your data with Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access 2 (WPA2).
- Passwords protect your Wi-Fi router with one that is strong and different from the password of your cameras.
- Change the default settings and passwords on your camera before first use.
- Ensure that your cameras have a strong password and two-factor authentication is set up.
- Enable the firewall that is built-in to your camera.
- Ensure that your firmware is up to date regularly.
- Turn the cameras off when you are home by using the camera's geofencing capabilities.

24.4 Additional Security Camera Information

For more information about each camera visit the links in the chart below. To read more information on each of the features discussed above or best practices for safeguarding your home security cameras visit the links below the chart.

Camera	URL
Wyze Cam V3	Wyze Cam v3 | Wired Security Camera
Google Nest Cam IQ Indoor	Nest Indoor & Outdoor Smart Security Cameras - Google Store
CYNC Indoor Cam	CYNC Smart Cameras (gelighting.com)
Eufy Security Indoor Cam 2K Pan and Tilt	eufy Security Indoor Cam 2K Pan & Tilt (eufylife.com)
D-Link DCS8300 Wi-Fi Camera	DCS-8300LHV2 Full HD Wi-Fi Camera | D-Link (dlink.com)
Simplisafe Simplicam	Wireless Security Camera System | SimpliSafe Indoor Security Camera
Arlo Essential Indoor Security Cam	Arlo Essential Indoor Security Camera for Inside Your Home | Arlo
Logitech Circle View	Logitech Circle View Camera Security System-HomeKit Enabled

25 MONEY SERVICES

Money services are unique in that their primary purpose is financial, but they also share attributes with social media, such as the ability to network and/or search for user profiles. Because the main service is financial, platform reviews and recommendations can tend to focus on security of finances, rather than privacy of personal information - but when a platform stores photos, "friends," comment history, home addresses, contact information, and more, you should protect your money service account the same way you would protect any of your other social media.

- A money service business is a non-bank institution that provides mechanisms for people to pay in any way or obtain money or cash in exchange for payment through a financial institution or institution.[481]
- An MSB provides a significant financial service to underdeveloped regions, often with limited or no banking services such as a small organization with outlets such as markets, pharmacies, and retailers.[482]
- In the United States and many other countries throughout the globe, regulations around money transmission are serious business as transmitting money is a serious business.

25.1 MONEY SERVICES SECURITY AND PRIVACY CONTROLS

When it comes to Money Services that are available to use, there are an ever-growing plethora of choices that offer unique ways to keep your money moving. The following links below provide you with the security and privacy settings a user can configure to reduce their Digital Exhaust.

Platform	Privacy Settings Link
PayPal Security	https://www.paypal.com/us/webapps/mpp/paypal-safety-and-security
PayPal Privacy	https://www.paypal.com/myaccount/privacy
Venmo Security and Privacy	https://venmo.com/account/settings/profile
CashApp Security	https://cash.app/help/us/en-us/1015-account-settings
CashApp Privacy	https://cash.app/legal/us/en-us/privacy
Braintree Security	https://www.braintreepayments.com/faq
Braintree Privacy	https://braintree.com/docs/privacy_policy.html
Google Pay Security	https://safety.google/intl/en_us/pay/
Google Pay Privacy	https://payments.google.com/legaldocument?family=0.privacynotice&hl=en-GB
Apple Pay Security	https://support.apple.com/en-us/HT203027
Apple Pay Privacy	https://support.apple.com/en-us/HT210665
Amazon Pay Security	https://paymentservices.amazon.com/docs/EN/51.html
Amazon Pay Privacy	https://paymentservices.amazon.com/privacy
Masterpass Security	https://masterpass.com/en-jp/faqs/manage-account-security.html
Masterpass Privacy	https://wallet.masterpass.com/Wallet/masterpass/en-au/privacy.html

25.1.1 PayPal Privacy Settings

PayPal's account data and privacy settings allow users to manage the use of PayPal to make payments on other apps and websites. Within the data and privacy settings, users can also turn off various cookies and control settings such as reminders and advertisements.[483]

25.1.2 Setting Payments To Private

By default, any time you pay for something through Venmo, that amount, and description are public and shown to your other friends on the app. Here is how to make it private.

- In the smartphone app, click on the profile icon, then the settings icon (looks like a gear). Select **Privacy** and set the Default Privacy Settings to **Private** (not **Public** or **Friends**).

25.1.3 Hide Past Transactions

You will have made an added privacy tweak to hide your past Venmo payments.

- In the same screen, scroll down to **More** and click **Past Transactions**. Tap on **Change All to Private**.

25.2 "TIPPING" ON TWITTER

In May 2021, Twitter integrated a PayPal "Tip Jar" system into Twitter's website, only to receive concerns from users when it was found that Tip Jar revealed the sender's address during each transaction. [484]

- This meant that any Twitter user who "tipped" another user could unknowingly reveal where they live.
- Fortunately, this risk can be mitigated by users selecting **No Address Needed** as an option when they send someone a "tip" on Twitter.[485]

25.3 VENMO PRIVACY SETTINGS

Venmo, which is owned by PayPal,[486] offers privacy settings for your transaction history as well as your user account, but it should be noted that most information is set to **public** by default.[487]

- Also of note, any user information sent to Venmo is accessible to PayPal as well.[488]

25.3.1 Venmo Transaction Settings

- **Public:** The transaction will be shared on the public feed and anyone on the internet may be able to see it.
- **Friends only:** The transaction will only be shared with your Venmo friends and with the other participant's Venmo friends.
- **Private:** Venmo will not share the transaction anywhere other than the **Your Stories** tab in the personal transactions feed and, if it is a payment to another user, the feed of the other person in the payment.

25.3.2 Sender/Recipient Payment Information

The payment amount, payment note, names of sender/recipient, and timestamp of the payment are available to everyone involved in the payment.

- ONLY the sender of the payment has access to the payment method used (for example: the bank account, debit/credit card number, etc.). The recipient will NEVER see this information.

25.3.3 Visibility Of Payment Information

When a payment is shared, the payment notes, names of sender/recipient, and timestamp of the payment will be visible on the public feed.

- ONLY the sender and recipient have access to the payment amount.
- ONLY the sender of the payment has access to the payment method used.

25.3.4 Sharing Venmo Payments

You can set the privacy setting on a payment or purchase on an individual basis. If you do not want to change the privacy setting every time you make a payment, you can change your default privacy setting. Your future payments will automatically default to your preference, but you can adjust this before completing the payment. See instructions below on how to change your privacy setting.

- When you transact with someone else on Venmo, including payouts from merchants or payments with business profiles, the more restrictive privacy setting between the two of you will be honored. If you have your payments set to Private but your friend has their payments set to Public, a payment between the two of you will be set to Private.
- Purchases made using your Venmo Mastercard Debit Card or Venmo Credit Card, and purchases from approved merchants when you pay with Venmo are Private by default, but you can change the privacy setting on any purchase to share them.
- All your transactions, regardless of privacy setting, will still be visible in your personal transactions feed so that you have a transaction record.

25.3.5 Privacy Settings Individual Payments

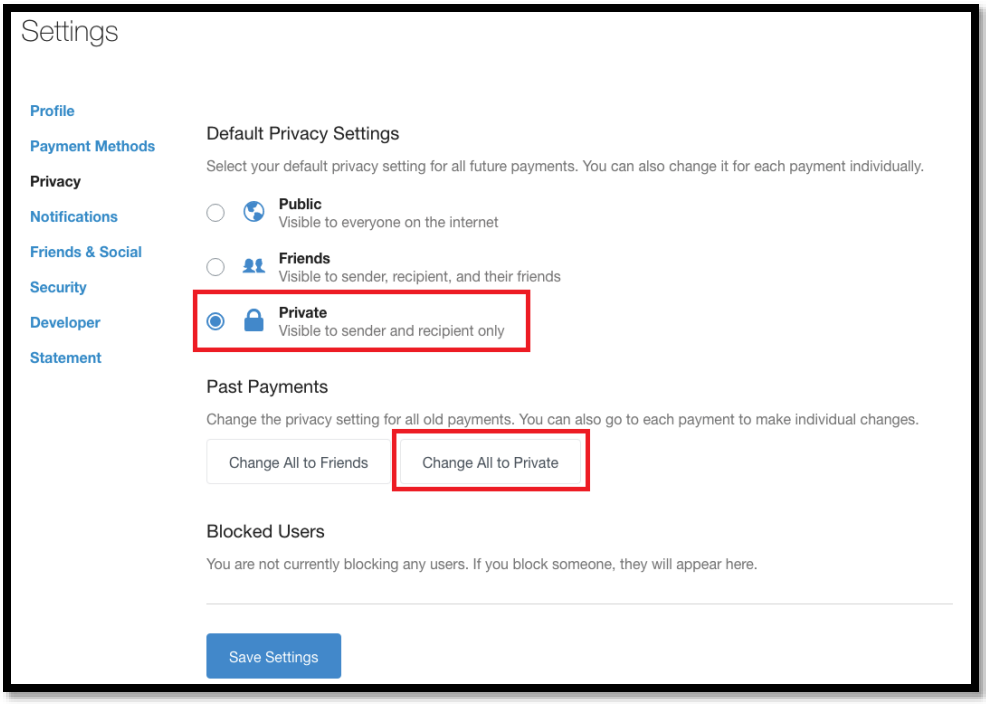
You can set the privacy setting for each individual payment or purchase, right from the payment or buy itself.

- Just select or tap on the privacy setting in any payment or purchase and select your preferred setting.
- Venmo's privacy webpage explains that transactions where each party has different settings, the more restricted setting will always be used[489]—so ensure you are protected by changing your default privacy setting to "private".

25.3.6 Hiding Past And Future Transactions

If you have not been setting individual transactions to **Private** as you go, you can still hide your entire history with a few clicks.

- First navigate to your home page, then select **Settings** from the sidebar.
- From Settings, select **Privacy**.
- Once on your Privacy Settings page, set your Default Privacy Settings to **Private**. To hide your entire transaction history, select **Change All to Private** in the **Past Payments** section.


Settings
Profile
Payment Methods
Privacy
Notifications
Friends & Social
Security
Developer
Statement
Default Privacy Settings
Select your default privacy setting for all future payments. You can also change it for each payment individually.
Public
Visible to everyone on the internet
Friends
Visible to sender, recipient, and their friends
Private
Visible to sender and recipient only
Past Payments
Change the privacy setting for all old payments. You can also go to each payment to make individual changes.
Change All to Friends
Change All to Private
Blocked Users
You are not currently blocking any users. If you block someone, they will appear here.
Save Settings

26 MOBILE WALLETS

Many consumers use their smartphones, tablets, and other mobile devices as mobile wallets to pay for goods and services, using apps to make both online and in-person purchases.[490] As our use of mobile payment services increases, so does the need to protect mobile devices, apps and associated data from theft and cyber-attacks.[491]

26.1 SAFEGUARDING YOUR MOBILE WALLET

- Never leave your smartphone unattended in a public place or visible in an unattended car.
- Consider your surroundings and use your smartphone or mobile device discreetly.
- Never use mobile payment services over an unsecured Wi-Fi network.
- Choose unique passwords for all your mobile apps.
- Install and keep security software on your smartphone. Apps are available to:
- Locate your smartphone from any computer.
- Lock your smartphone to restrict access.
- Wipe sensitive personal information and mobile wallet credentials from your smartphone when trading in your device.
- Be careful about using social networking apps, which may pose a security risk and may allow unwanted access to personal information, including your mobile financial data.
- Monitor financial accounts linked to in mobile apps for any fraudulent charges.
- Review the service agreements for these accounts to find out what steps to take if your smartphone is lost, stolen, or hacked, and what charges a user may be responsible for paying.[492]

26.2 IF YOUR MOBILE DEVICE IS LOST/STOLEN

- If you are not certain whether your smartphone or mobile device has been stolen, or if you have simply misplaced it, try finding the smartphone by calling it or by using the security software's GPS locator.
- If you have installed security software on your smartphone, use it to lock the device, wipe sensitive personal information and/or activate the alarm.
- Immediately report the theft or loss to your wireless carrier. If you provide your carrier with the IMEI or MEID number, your carrier may be able to disable your smartphone and mobile payment apps, and block access to your personal information and sensitive data. Request written confirmation from your carrier that you reported the smartphone as missing and that the smartphone was disabled.
- Report the theft to the police including the make and model, serial and either the International Mobile Equipment Identifier (IMEI) or the Mobile Equipment Identifier (MEID) number in your report.
- Some service providers need proof that the smartphone was stolen, and a police report can provide that documentation.[493]
- Your service provider may be able to use your IMEI or MEID or ESN number to disable your device and block access to the information it carries.

- Some phones display the IMEI/MEID number when you dial *#06#. The IMEI/MEID also can be found on a label located beneath the phone's battery or on the box that came with the phone.
- The police may need your smartphone's unique identifying information if it is stolen or lost. Write down the make, model number, serial number, and unique device identification number - either the IMEI or MEID number.
- If you are unable to lock your stolen or lost smartphone, change all your passwords for mobile payment apps and any bank or credit card accounts that you have accessed using your smartphone service, then contact those financial institutions about the loss or theft.

27 PHOTO METADATA

Photo metadata are set of data describing and supplying information about rights and administration of an image.

- Many devices with cameras, like smartphones, embed the set of data into the pictures they capture.
- Data types include the shutter speed, ISO, aperture data, camera mode, and/or GPS location of where the picture was taken.
- They are stored within the pictures they take in a format called the Exchangeable Image Format (EXIF) and left intact, present a potential privacy vulnerability when shared across devices or uploaded onto the Internet. In short, to protect your privacy, remove EXIF data from your images.

27.1 iOS

27.1.1 Remove EXIF Data

Prior to Apple's release of iOS 13 there was no native way to disable EXIF data.

- With the release of iOS 14, Apple now supplies users a way to remove EXIF data from photos. This **URL** will inform you on how to do so along with other key features within iOS 15 that will better enhance your privacy.[494]
- However, apps, which can remove EXIF data, are available in the iOS App Store.
- One such app includes Exif Data and the pro version costs $0.99/year. It enables you to view, edit, and remove metadata from your iOS devices like iPhone and iPad.
- It also allows you to spoof a location of your choosing of where the photo was taken which will appear within the photo's metadata.

Figure 7. Icon for Exif Metadata Apo

27.1.2 EXIF iOS photos on Apple Mac

The following **URL** is extremely informative[495]:

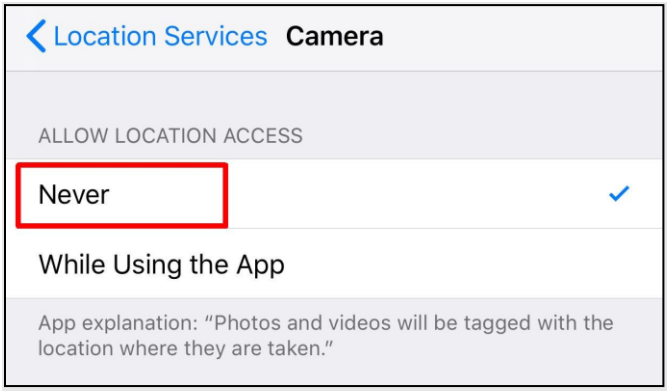
- The easiest way to view EXIF data is on your Mac. Just transfer your photos to your Mac using **iPhoto**, tap on the image and select the **i** for info.
- All the EXIF data, including a map of the GPS coordinates will appear within the iPhoto window.

- If you do not see a map, then you may have to hop into **iPhoto preferences** and **turn on** this mapping feature. **Go to iPhoto > Preferences > Advanced**. If you choose **"Automatically"**, then iPhoto will scan your photos for GPS data and map them for you.
- While you are in the settings, you should check the status of the **Include location information for published photos** option.
- If it is selected, then the location data will remain intact when you use iPhoto to upload your photos to other services.
- If it is not selected, then the location data will be stripped from the file by iPhoto during the upload process.
- Unselecting this option is the preferred choice if you don't want people to know the location of your photos.

27.1.3 EXIF Location Data on iOS

Turn off photo geotagging feature by going to **Location Services** in the **Settings**.

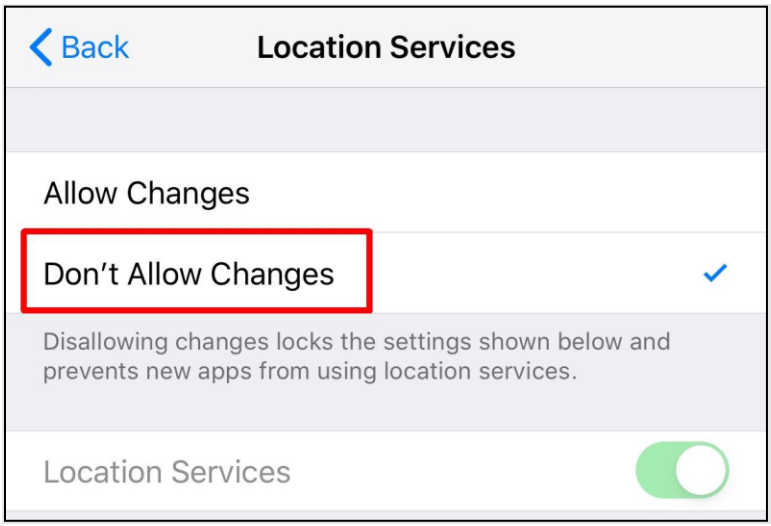
- Tap on **Settings > Privacy > Location Services** and then scroll down to the **Camera app** to make sure it is toggled off.
- NOTE: this only applies to photos taken after you have turned off the location feature and does not remove any other EXIF data.



27.1.4 iOS App Change Camera Settings

Enable Screen Time for your devices, go to **Location Services**, and click **Don't Allow changes**.

- See Section 3.18.1 for more information about Screen Time.
- You can also visit Apple's information about Screen Time at the following **URL**.[496]



27.2 ANDROID

27.2.1 Camera App Location Data

Open the **Camera app** on your phone.

- Tap the **Settings** option on the viewfinder. For Samsung phones, the settings gear is in the top left corner. For Google Pixel phones, you will need to tap the downward-facing arrow at the top of the screen, then tap the settings gear in the menu that appears.
- Turn off the **Location** toggle in the setting menu. On Samsung phones, **Location** is near the bottom, but it is the first setting in **Google Camera** advanced menu.[497]

27.2.2 Gallery App Location Data

Open **Gallery app** on your phone.

- Tap the **picture** you want to remove location data from.
- **Swipe up** on the picture to pull up the picture's information.
- Tap **Edit**.
- Tap the **red minus** next to the location data to remove it.
- Tap **Save**.

27.3 GOOGLE PHOTOS

There is an obvious concern any time you upload your pictures to a service on the internet you should exercise caution.[498] Even though Google actively works to secure their services, there is always a chance

of vulnerability and the risk that someone could get access to your pictures and videos. The following privacy settings are worth noting should you choose to enable them:

- Only share pictures with people you know.
- Check the **Sharing** settings on each album you create.
- Do not upload pictures to Shared Albums from people you do not know.
- Turn on **Remove Geo-Location in Items Shared by Link**.
- Turn off **Google Location History** in the Google Photos Settings.
- Occasionally check the Sharing settings on your account to keep things private.

Beyond what was noted above, Google has other specific privacy settings available with Google Photos.

27.3.1 Location Data In Photos

Open **Google Photos** on your phone or visit the **Google Photos website** on your computer.[499]

- Open the **picture** you wish to remove location data from.
- In the **Google Photos** app, swipe up to reveal the photo information. On desktop, click the **Info** icon in the top right option bar (looks like a lower case *i* in a circle).
- Tap the icon to the right of the listed location.
- In the **Google Photos** app, tap **Remove Location**. On desktop, click **No location**.
- In the **Google Photos** app, tap **Remove**.

27.3.2 Memories

Memories are collections of some of your best photos and videos whether from previous years or recent weeks. **Memories** are available on Android devices, iPhones, and iPads.

You can select the types of **Memories** you want to see above your photo grid. The Memories carousel above the photo grid only appears when at least one memory type is selected.[500]

- On your Android phone or tablet, open the **Photos** app.
- At the top right, tap your **account profile photo** or initial and then Photo's settings and then **Memories**.
- Tap **Featured Memories**.
- Select the types of memories you want to see.

27.3.3 Hide someone

Google allows you to exclude people and even pets from **Memories**.[501]

- On your Android phone or tablet, open the **Photos** app.
- At the top right, tap your account profile photo or initial and then Photo's settings and then **Memories**.
- Tap **Hide** people & pets.
- Choose who you want to hide.
- To show someone, tap their face again.

28 ENDNOTES

[1] Website | Cybersecurity and Infrastructure Security Agency | "TRAFFIC LIGHT PROTOCOL (TLP) DEFINITIONS AND USAGE" | **https://www.cisa.gov/tlp** | accessed on 19 May 2022
[2] Website | Forum of Incident Response and Security Teams, Inc. | "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0" | **https://www.first.org/tlp/** | accessed on 19 May 2022
[3] Website | Forum of Incident Response and Security Teams, Inc. | "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0" | **https://www.first.org/tlp/** | accessed on 19 May 2022
[4] Website | Forum of Incident Response and Security Teams, Inc. | "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0" | **https://www.first.org/tlp/** | accessed on 19 May 2022
[5] Website | Forum of Incident Response and Security Teams, Inc. | "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0" | **https://www.first.org/tlp/** | accessed on 19 May 2022
[6] Website | DigitalElement.com | "Digital Data Exhaust – 2018 Research Results" | 2021 | **https://www.digitalelement.com/digital-data-exhaust/** | accessed on 20 June 2021.
[7] Online article | Norton | "How Data Brokers Find and Sell Your Personal Info" | 18 January 2021 | **https://us.norton.com/internetsecurity-privacy-how-data-brokers-find-and-sell-your-personal-info.html** | accessed on 22 July 2021.
[8] Online article | TechCrunch | "The Power of Data Exhaust" | 26 May 2013 | **https://techcrunch.com/2013/05/26/the-power-of-data-exhaust/** | accessed on 20 June 2021.
[9] Online article | CultureBy – Grant McCracken | "How Social Networks Work: The Puzzle of Exhaust Data" | 19 July 2007 | **https://cultureby.com/2007/07/how-social-netw.html** | accessed on 20 June 2021.
[10] Online Editorial | Ghostery | "Tracking the Trackers 2020: Web Tracking's Opaque Business Model of Selling Users" | 2020 | **https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users** | accessed on 19 June 2022
[11] Online article | Medium | "Your Data is a Myth" | 11 June 2020 | **https://medium.com/swlh/your-data-is-a-myth-37997abcc82a**
[12] Online article | TNW | "Here's how we take back control over our digital identities" | 24 November 2018 | **https://thenextweb.com/news/heres-how-we-take-back-control-over-our-digital-identities** | accessed on 27 July 2021.
[13] Online Article | Norton | "The privacy paradox: How much privacy are we willing to give up online?" | April 14, 2021 | **https://us.norton.com/internetsecurity-privacy-how-much-privacy-we-give-up.html** | accessed on 19 June 2022
[14] Online article | Privacy News Online | "When the Home is no Data Protection Haven: Addressing Privacy Threats from Intimate Relationships" | 12 June 2020 | **https://www.privateinternetaccess.com/blog/?p=13298** | accessed on 20 June 2021.
[15] Online Editorial | Ghostery | "Clean up your Digital Footprint" | 2021 | **https://www.ghostery.com/blog/clean-up-your-digital-footprint** | accessed on 19 June 2022
[16] Online Article | World Economic Forum | "Digital privacy comes at a price. Here's how to protect it" | September 8, 2021 | **https://www.weforum.org/agenda/2021/09/how-to-protect-digital-privacy/** | accessed on 19 June 2022
[17] Online Editorial | Ghostery | "Clean up your Digital Footprint" | 2021 | **https://www.ghostery.com/blog/clean-up-your-digital-footprint** | accessed on 19 June 2022
[18] Online article | Visual Capitalist | "The Multi-Billion Dollar Industry That Makes Its Living from Your Data" | 14 April 2018 | **https://www.visualcapitalist.com/personal-data-ecosystem/** | accessed on 22 June 2021.
[19] Online article | Tech Target | "The Wide Web of Nation-State Hackers Attacking the US" | 20 April 2021 | **https://searchsecurity.techtarget.com/news/252499613/The-wide-web-of-nation-state-hackers-attacking-the-US** | accessed on 30 July 2021.
[20] Online article | Medium | "Targeted Threat Intelligence, generated from Open-Source Information" | 1 June 2020 | **https://alex-newman.medium.com/targeted-threat-intelligence-generated-from-open-source-information-e13a3a2c58dd** | accessed on 30 July 2021.
[21] Online article | Norton | "The Privacy Paradox: How Much Privacy Are We Willing to Give Up Online?" | 14 April 2021 | **https://us.norton.com/internetsecurity-privacy-how-much-privacy-we-give-up.html** | accessed on 2 August 2021.
[22] Blog post | Data Privacy | "What is Personally Identifiable Information (PII) and What is Personal Data?" | 23 February 2021 | **https://dataprivacymanager.net/what-is-personally-identifiable-information-pii/** | accessed on 2 August 2021.
[23] Online article | Techcrunch | "Data Was The New Oil, Until The Oil Caught Fire" | 2 May 2021 | **https://techcrunch.com/2021/05/02/data-was-the-new-oil-until-the-oil-caught-fire/** | accessed on 2 August 2021.
[24] Online article | Digital Journal | "Digital Identity and Privacy Issues are Worrying Consumers More Than Ever" | 15 May 2021 | **https://www.digitaljournal.com/tech-science/digital-identity-and-privacy-issues-are-worrying-consumers-more-than-ever/article** | accessed on 2 August 2021.
[25] Online article | Gizmodo | "How to Track the Tech That's Tracking You Every Day" | 6 June 2020 | **https://gizmodo.com/how-to-track-the-tech-thats-tracking-you-every-day-1843908029** | accessed on 2 August 2021.
[26] Online article | MySudo | "What is Digital Exhaust and Why Does it Matter?" | 17 August 2020 | **https://mysudo.com/2020/08/what-is-digital-exhaust-and-why-does-it-matter/** | accessed on 2 August 2021.

[27] Blog post | Epam | "The Privacy Web: A Look into Where Personal Data Protection Stands Today and Where It's Headed" | 7 October 2020 | https://www.epam.com/insights/blogs/the-privacy-web-personal-data-protection-today-and-where-its-headed | accessed on 2 August 2021.
[28] Online article | Forbes | "Four Steps to Take Control of Your Privacy Management" | 30 March 2020. https://www.forbes.com/sites/forbestechcouncil/2020/03/30/four-steps-to-take-control-of-your-privacy-management/?sh=2fd953004761
[29] Online article | The Register | "Bad News: So Much of Your Personal Data has Been Hacked that Lesson Manuals on How To Use It are the Latest Hot Property" | 16 April 2020 | https://www.theregister.com/2020/04/16/cybercrimeby_fraud_lessons/ | accessed on 23 July 2021.
[30] Online Article | The State and Future of GEOINT 2017 Report | "Activity-Based Intelligence: Understanding Patterns-of-Life" | April 18, 2017 | https://medium.com/the-state-and-future-of-geoint-2017-report/activity-based-intelligence-understanding-patterns-of-life-481c78b7d5ae | accessed on 19 June 2022
[31] Online Article | Forensic Focus for Digital Forensics & E-Discovery Professionals | "Forensic Pattern of Life Analysis" | February 25, 2020 | https://www.forensicfocus.com/articles/forensic-pattern-of-life-analysis/ | accessed on 19 June 2022
[32] Online Article | Investopedia | "Mobile Advertising" | November 11, 2020 | https://www.investopedia.com/terms/m/mobile-advertising.asp | accessed on 19 June 2022
[33] Online Article Glossary | Hotjar | "CRO glossary: Behavioral targeting" | https://www.hotjar.com/conversion-rate-optimization/glossary/behavioral-targeting/ | accessed on 19 June 2022
[34] Online Article Glossary | Social Protection.Org | "What is Social Protection?" | Oct 2017 | https://socialprotection.org/learn/glossary/categorical-targeting-targeting-method | accessed on 19 June 2022
[35] Online Article | Intuit Mailchimp | "What is Retargeting?" | https://mailchimp.com/resources/what-is-retargeting/ | accessed on 19 June 2022
[36] Online Article | Choozle | "What is: Search Retargeting?" | June 16, 2020 | https://choozle.com/blog/search-retargeting/ | accessed on 19 June 2022
[37] Online Article | HubSpot | "A Marketer's Quick Guide to Dynamic Ads" | January 11, 2022 | https://blog.hubspot.com/marketing/dynamic-ads | accessed on 19 June 2022
[38] Online Article | WebKit | "Tracking Prevention in WebKit" | https://webkit.org/tracking-prevention/ | accessed on 19 June 2022
[39] Online Article | Fast Company | "Credit card Companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism" | May 12, 2020 | https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism | accessed on 19 June 2022
[40] Online article | Cloudflare | "Why is HTTP not secure? HTTP vs. HTTPS" | https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/ | accessed on 12 May 2022
[41] Blog post | GlobalSign | "What's the difference between HTTP and HTTPS?" | 22 May 2018 | https://www.globalsign.com/en/blog/the-difference-between-http-and-https
[42] Online Article | CHRON | "How to Get Rid of a Red Line Through HTTPS" | https://smallbusiness.chron.com/tell-website-using-ssl-53686.html | accessed on 19 June 2022
[43] Online article | AddExchanger | "Oracle Signs On To Support Unified ID 2.0" | 13 May 2021 | https://www.adexchanger.com/online-advertising/oracle-signs-on-to-support-unified-id-2-0/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ad-exchange-news+%28AdExchanger.com%3A+Exchanging+Ideas+On+Digital+Media+Optimization%29 | accessed 22 July 2021.
[44] Online article | TechCrunch | "Oracle's BlueKai Tracks You Across the Web. That Data Spilled Online" | 19 June 2020 | https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ | accessed on 22 July 2021.
[45] Online article | Digiday | "Digiday Guide: Everything You Need to Know About the End of the Third-Party Cookie" | 6 May 2020 | https://digiday.com/media/digiday-guide-everything-you-need-to-know-about-the-end-of-the-third-party-cookie/ | accessed on 30 July 2021.
[46] Online Article | Who Tracks Me | "Third-party cookies – the guests who won't leave" | August 27, 2018 | https://whotracks.me/blog/block-third-party-cookies.html | accessed on 19 June 2022
[47] Online Article | Who Tracks Me | "Third-party cookies – the guests who won't leave" | August 27, 2018 | https://whotracks.me/blog/block-third-party-cookies.html | accessed on 19 June 2022
[48] Online Article | ZD Net | "Cybersecurity 101: Protect your privacy from hackers, spies, and the government" | 21 January 2022 | https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/
[49] Online article | PrivacyBee | https://privacybee.com/blog/what-is-browser-fingerprinting-and-how-do-i-prevent-it/ | accessed on 4 October 2021
[50] Online article | TNW | "Digital Fingerprints are the New Cookies — and Advertisers Want Yours" | 2 April 2020 | https://thenextweb.com/news/digital-fingerprints-are-the-new-cookies-and-advertisers-want-yours | accessed on 25 June 2022
[51] Online Article | Who Tracks Me | "Fingerprinting" | July 22, 2017 | https://whotracks.me/blog/fingerprinting.html | accessed on 19 June 2022

[52] Online article | Privacy News Online | "Mozilla Study Reaffirms that Internet History Can be Used for "Reidentification"" | 31 August 2020 |**https://www.privateinternetaccess.com/blog/mozilla-study-reaffirms-that-internet-history-can-be-used-for-reidentification/** | accessed on 25 July 2021.
[53] Online article | HackRead | "Cross-browser Tracking Vulnerability Compromises User Anonymity" | 17 May 2021 | **https://www.hackread.com/cross-browser-tracking-compromises-user-anonymity/**| accessed on 25 July 2021.
[54] Online article | Privacy Bee | "What is device fingerprinting and how do I prevent it?" | **https://privacybee.com/blog/what-is-device-fingerprinting-and-how-do-i-prevent-it/** | accessed on 25 June 2022
[55] Website | Amazon | "Browser Extensions & Privacy" | **https://www.amazon.com/gp/help/customer/display.html?nodeId=G8V457F4P763VW8D** | 25 August 2021.
[56] Online article | Google | "Install and manage extensions" | **https://support.google.com/chrome_webstore/answer/2664769** | accessed on 19 May 2022
[57] Online article | Mozilla Foundation | "Disable or remove Add-ons" | **https://support.mozilla.org/en-US/kb/disable-or-remove-add-ons** | accessed on 19 May 2022
[58] Online article | Apple Inc. | "How to install Safari extensions on your Mac" | **https://support.apple.com/en-us/HT203051** | 14 November 2019
[59] Online article | Microsoft | "Find, add, or remove extensions in Microsoft Edge" | **https://support.microsoft.com/en-us/microsoft-edge/find-add-or-remove-extensions-in-microsoft-edge-f3522273-d067-7435-6a9d-fdb99213e9a8** | accessed on 19 may 2022
[60] Online article | Opera Software | "Opera Help - Add Chrome extensions to Opera" | **https://help.opera.com/en/latest/customization/#extensions** | accessed on 19 May 2022
[61] Online article | TechCrunch | "Who Gets to Own Your Digital Identity?" | 22 August 2019 | **https://techcrunch.com/2019/08/22/who-gets-to-own-your-digital-identity/**| accessed on 27 July 2021.
[62] Online article | MacRumors | "A Day in the Life of Your Data: Apple Details How Companies Can Track You Across Apps and Websites" | 27 January 2021 | **https://www.macrumors.com/2021/01/28/apple-a-day-in-the-life-of-your-data/**| accessed on 30 July 2021.
[63] Website | The Association of National Advertisers | "ANA Driving Growth" | **https://www.ana.net/about** | accessed on 10 May 2022
[64] Online article | Digiday | "Question of the Day: How are Publishers Using Contextual Data?" | 2021 | **https://digiday.com/sponsored/question-of-the-day-how-are-publishers-using-contextual-data/**| accessed on 30 July 2021.
[65] Online article | EFF | "Protecting Your Privacy if Your Phone is Taken Away" | 4 June 2020 | **https://www.eff.org/deeplinks/2020/06/protecting-your-privacy-if-your-phone-taken-away**| accessed on 20 July 2021.
[66] Online article | HackRead | "How to Protect Your Privacy on a Smartphone: 12 Tips & Tricks" | 17 June 2021 | **https://www.hackread.com/how-to-protect-privacy-smartphone-12-tips-tricks/**| accessed on 20 July 2021.
[67] Online article | Prey | "Phone Security: 20 Ways to Secure Your Mobile Phone" | 6 April 2021 | **https://preyproject.com/blog/en/phone-security-20-ways-to-secure-your-mobile-phone/**| accessed on 20 July 2021.
[68] Online Document | National Nuclear Security Agency | "Mobile Device Best Practices" | **https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF** | accessed 19 June 2022
[69] Online article | Wired | "Mobile Websites Can Tap into Your Phone's Sensors Without Asking" | 26 September 2018 | **https://www.wired.com/story/mobile-websites-can-tap-into-your-phones-sensors-without-asking**| accessed on 30 June 2021.
[70] Online article | Gizmodo | "All the Sensors in Your Smartphone, and How They Work" | 29 June 2020 | **https://gizmodo.com/all-the-sensors-in-your-smartphone-and-how-they-work-1797121002**| accessed on 30 June 2021.
[71] Online article | Lifehacker | "It's Time to Check Which Apps Are Tracking Your Location" | 10 December 2018 | **https://lifehacker.com/its-time-to-check-which-apps-are-tracking-your-location-1830979707**| accessed on 30 June 2021.
[72] Journal article | *Science News*, Volume 193, Number 2 | "The Spy in Your Pocket" | 3 February 2018 | **https://www.sciencenews.org/sn-magazine/february-3-2018** | accessed on 5 July 2021.
[73] Online article | Digital Trends | "How to Track a Phone Using Android or iOS" | 21 March 2021 | **https://www.digitaltrends.com/mobile/how-to-track-a-cell-phone/**| accessed on 30 June 2021.
[74] Online article | Lifehacker | "It's Time to Check Which Apps Are Tracking Your Location" | 10 December 2018 | **https://lifehacker.com/its-time-to-check-which-apps-are-tracking-your-location-1830979707**| accessed on 30 June 2021.
[75] Blog post | AppCensus | "Ad IDs Behaving Badly" | 14 February 2019 | **https://blog.appcensus.mobi/2019/02/14/ad-ids-behaving-badly**| accessed 30 June 2021.
[76] Online article | Lifehacker | "PSA: Your Phone Logs Everywhere You Go. Here's How to Turn It Off" | 9 August 2019 | **https://lifehacker.com/psa-your-phone-logs-everywhere-you-go-heres-how-to-t-1486085759|** accessed on 30 June 2021.
[77] Online article | Gizmodo | "How Location Tracking Actually Works on Your Smartphone" | 3 September 2018 | **https://gizmodo.com/how-location-tracking-actually-works-on-your-smartphone-1828356441** | accessed on 30 June 2021.
[78] Blog post | BuzzFeed | "A Lot of Apps Sell Your Data. Here's What You Can Do About It" | 1 May 2018 | **https://www.buzzfeednews.com/article/nicolenguyen/how-apps-take-your-data-and-sell-it-without-you-even**| accessed on 30 June 2021.

[79] Online Article | CNet | “The Data Privacy Tips Digital Security Experts Wish You Knew” | 03 May 2022 | https://www.cnet.com/tech/services-and-software/what-digital-security-experts-wish-you-knew-about-data-privacy/
[80] Website | FCC | “FCC Smartphone Security Checker” | https://www.fcc.gov/smartphone-security | 30 October 2015
[81] Online article | Make Use Of | “How Do Websites Track Your Online Activities?” | 22 May 2021 | https://www.makeuseof.com/how-do-websites-track-your-online-activities/ | accessed on 24 July 2021.
[82] Online article | “Now Sites Can Fingerprint You Online Even When You Use Multiple Browsers” | 13 February 2017 | https://arstechnica.com/information-technology/2017/02/now-sites-can-fingerprint-you-online-even-when-you-use-multiple-browsers/| accessed 24 July 2021.
[83] Blog post | Intego | “Understanding Safari’s New Privacy Report” | 24 September 2020 | https://www.intego.com/mac-security-blog/understanding-safaris-new-privacy-report/
[84] Blog post | Intego | “Understanding Safari’s New Privacy Report” | 24 September 2020 | https://www.intego.com/mac-security-blog/understanding-safaris-new-privacy-report/
[85] Online article | Apple Inc. | “About App Privacy Report” | 13 December 2021 | https://support.apple.com/en-us/HT212958
[86] Online article | 9 To 5 Mac | “How to see what apps are doing in the background with iPhone App Privacy Report” | 14 December 2021 | https://9to5mac.com/2021/12/14/how-to-turn-on-iphone-app-privacy-report/
[87] Blog post | Intego | “Understanding iOS and iPadOS App Privacy Report” | 14 December 2021 | https://www.intego.com/mac-security-blog/understanding-ios-and-ipados-app-privacy-report/
[88] Website | MacRumors | "iOS 15: How to Hide Your IP Address From Trackers in Safari" | https://www.macrumors.com/how-to/hide-your-ip-address-from-trackers-ios/ | accessed on 1 October 2021
[89] Website | FastCompany | "Use these 8 new iOS 15 privacy and security features right away" | https://www.fastcompany.com/90673312/ios-15-iphone-privacy-security-features | accessed on 1 October 2021
[90] Online article | Apple Inc. | “Preventing Insecure Network Connections” | https://developer.apple.com/documentation/security/preventing_insecure_network_connections | accessed on 11 May 2022
[91] Online article | iDrop News | “Everything You Need to Know About Apple’s Private Relay” | 1 December 2021 | https://www.idropnews.com/news/everything-you-need-to-know-about-apples-private-relay/172471/
[92] Online article | Apple Inc. | “Turn on iCloud Private Relay on iPhone” | https://support.apple.com/guide/iphone/turn-on-icloud-private-relay-iph499d287c2/ios | accessed on 11 May 2022
[93] Online article | Apple Inc. | “Sign in with your Apple ID” | https://support.apple.com/guide/iphone/aside/iph39beaede9/15.0/ios/15.0 | accessed on 11 May 2022
[94] Website | MacRumors | "Apple Putting a Stop to Email Tracking Pixels With Mail Privacy Protection in iOS 15 and macOS Monterey" | https://www.macrumors.com/2021/06/10/ios-15-mail-privacy-protection-tracking-pixels/ | accessed on 1 October 2021
[95] Online article | Apple Inc. | “About communication safety in Messages” | 13 December 2021 | https://support.apple.com/en-us/HT212850
[96] Online article | Apple Inc. | “Expanded Protections for Children” | https://www.apple.com/child-safety/ | accessed on 11 May 2022
[97] Online article | Apple Inc. | “Use parental controls on your child's iPhone, iPad, and iPod touch” | 19 November 2021| https://support.apple.com/en-us/HT201304
[98] Online article | Apple | "Set a passcode on iPhone" | https://support.apple.com/guide/iphone/set-a-passcode-iph14a867ae/ios | accessed on 1 October 2021
[99] Online article | Apple | "Two-factor authentication for Apple ID" | https://support.apple.com/en-us/HT204915 | accessed on 1 October 2021
[100] Website | Apple Inc. | “iTunes Store & Privacy” | https://www.apple.com/legal/privacy/data/en/itunes-store/ | accessed on 11 May 2022
[101] Website | U.S. Department of State | “High-Risk Area Travelers” | 6 November 2019 | https://travel.state.gov/content/travel/en/international-travel/before-you-go/travelers-with-special-considerations/high-risk-travelers.html
[102] Website | Apple Inc. | “Device Analytics & Privacy” | https://www.apple.com/legal/privacy/data/en/device-analytics/ | accessed on 11 May 2022
[103] Website | Apple Inc. | “iOS 15” | https://www.apple.com/ios/ios-15/ | accessed 11 May 2022
[104] Online Article | Apple Inc. | “Apple advances its privacy leadership with iOS 15, iPadOS 15, macOS Monterey, and watchOS 8” | 07 June 2021 | https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/
[105] Online article | Digiday | “The Elephant in the Room: Companies Persist with Fingerprinting as a Workaround to Apple’s New Privacy Rules” | 12 April 2021 | https://digiday.com/media/the-elephant-in-the-room-companies-persist-with-fingerprinting-as-a-workaround-to-apples-new-privacy-rules/ | accessed on 8 August 2021.
[106] Online article | Apple Inc. | “Apple Advertising & Privacy” | 15 February 2022 | https://www.apple.com/legal/privacy/data/en/apple-advertising/
[107] Online article | Future of Privacy Forum | “Understanding the World of Geolocation Data” | 22 May 2020 | https://fpf.org/blog/understanding-the-world-of-geolocation-data/ | accessed on 30 July 2021.

[108] Online article | 9to5Mac | "iOS 14 Lets Users Grant Approximate Location Access for Apps That Don't Require Exact GPS Tracking" | 12 August 2020 | **https://9to5mac.com/2020/08/12/ios-14-precise-location/** | accessed on 30 July 2021.
[109] Press Release | NSA | "How Mobile Device Users Can Limit Their Location Data Exposure" | 4 August 2020 | **https://www.nsa.gov/news-features/press-room/Article/2298930/how-mobile-device-users-can-limit-their-location-data-exposure/** | accessed on 30 July 2021.
[110] Online article | Apple Inc. | "Location Services & Privacy" | 15 February 2022 | **https://www.apple.com/legal/privacy/data/en/location-services/**
[111] Online article | MacRumors | "Security Researchers Develop Framework for Tracking Bluetooth Devices Using Find My" | 4 March 2021 | **https://www.macrumors.com/2021/03/04/security-researchers-find-my-tracking-framework/** | accessed on 23 July 2021.
[112] Online article | How-To Geek | "What Is Apple's Find My Network?" | 9 May 2021 | **https://www.howtogeek.com/725842/what-is-apples-find-my-network/** | accessed 27 July 2021.
[113] Website | MacRumors | "iOS 15 Overview" | **https://www.macrumors.com/roundup/ios-15/** | accessed on 1 October 2021
[114] Online article | Android Authority | "Hands-on with Privacy Dashboard, One of Android 12's Best New Features" | 9 June 2021 | **https://www.androidauthority.com/android-privacy-dashboard-1233846/** | accessed on 5 August 2021.
[115] Online article | DefendingDigital | "Android Security And Privacy Guide 2021" | 2021 | **https://defendingdigital.com/android-security-privacy-guide/** | accessed on 5 August 2021.
116 Online article | DefendingDigital | "Android Security And Privacy Guide 2021" | 2021 | **https://defendingdigital.com/android-security-privacy-guide/** | accessed on 5 August 2021.
[117] Website | Support.Google.com | "Play Console Help" | 2021 | **https://support.google.com/googleplay/android-developer/answer/6048248?hl=en** | accessed on 8 August 2021.
[118] Online article | Android Authority | "Hands-on with Privacy Dashboard, One of Android 12's Best New Features" | 9 June 2021 | **https://www.androidauthority.com/android-privacy-dashboard-1233846/** | accessed on 5 August 2021.
119 Online article | Restore Privacy | "How to Secure Your Android Device and Have More Privacy" | 13 May 2020 | **https://restoreprivacy.com/secure-android-privacy/** | accessed on 5 August 2021.
[120] Online article | Defending Digital | "Google Account Security And Privacy Guide 2022" | **https://defendingdigital.com/google-account-security-privacy-guide/** | accessed on 11 May 2022
[121] Online article | Android Central | "How to remove location data from photos on Android" | 3 June 2020 | **https://www.androidcentral.com/how-remove-location-data-photos-android** | accessed on 8 August 2021.
[122] Online article | Android Central | "How to remove location data from photos on Android" | 3 June 2020 | **https://www.androidcentral.com/how-remove-location-data-photos-android** | accessed on 8 August 2021.
[123] Online article | How-to Geek | "What Is the Privacy Dashboard on Android?" | 14 June 2021 | **https://www.howtogeek.com/733712/what-is-the-privacy-dashboard-on-android/** | accessed on 5 August 2021.
124 Online article | PrivacySavvy | "Disable Ad Tracking on All Your Devices: The Complete Guide with Screenshots" | 27 May 2021 | **https://privacysavvy.com/security/safe-browsing/disable-ad-tracking/** | accessed on 5 August 2021.
[125] Website | Support.Google.com | "Play Console Help" | 2021 | **https://support.google.com/googleplay/android-developer/answer/6048248?hl=en** | accessed on 8 August 2021.
[126] Online article | Defending Digital | "Secure Messaging In 2021: Everything You Need To Know" | **https://defendingdigital.com/email-and-text-messages-arent-secure-use-secure-messaging-instead/** | accessed on 11 May 2022
[127] Online article | How-To Geek | "The Best Android Phones of 2022" | 16 February 2022 | **https://www.howtogeek.com/734936/best-android-phones/**
[128] Online article | How-To Geek | "Why You Shouldn't Use Your ISP's Default DNS Server" | 14 April 2020 | **https://www.howtogeek.com/664608/why-you-shouldnt-be-using-your-isps-default-dns-server/**
[129] Online article | How-To Geek | "How to Search the Settings Menu on Android" | 26 June 2021 | **https://www.howtogeek.com/702648/how-to-search-the-settings-menu-on-android/**
[130] Online article | Google | "Teach Google Assistant to recognize your voice with Voice Match" | **https://support.google.com/assistant/answer/9071681** | accessed on 11 May 2022
[131] Website | Google | "Google Privacy Policy" | **https://policies.google.com/privacy** | accessed on 12 May 2022
[132] Online Article | Google Account Help | "Manage your Location History" | **https://support.google.com/accounts/answer/3118687?hl=en** | accessed on 26 June 2022
[133] Website | Google | "Help your family create healthy digital habits" | **https://families.google.com/familylink/** | accessed on 12 May 2022
[134] Website | Support.Google.com | "Play Console Help" | 2021 | **https://support.google.com/googleplay/android-developer/answer/6048248?hl=en** | accessed on 8 August 2021.
[135] Blog post | Google | "Get more information about your apps in Google Play" | 26 April 2022 | **https://blog.google/products/google-play/data-safety/**
[136] Online article | Google | "Get more information about your apps in Google Play" | 26 April 2022 | **https://blog.google/products/google-play/data-safety/**
[137] Website | Google | "Designing Apps for Children and Families" | **https://support.google.com/googleplay/android-developer/answer/9893335?hl=en** | accessed on 11 May 2022

[138] Online article | App Defense Alliance | "Mobile Application Security Assessment" | **https://appdefensealliance.dev/masa** | accessed on 11 May 2022
139 Online article | Fox News | "Lock Down Your Phone From Snoops and Hackers" | 12 June 2021 | **https://www.foxnews.com/tech/lock-down-phone-from-snoops-hackers** | accessed on 20 July 2021.
[140] Online article | Lifewire | "How to Test a Suspicious Link Without Clicking It" | 2 May 2022 | **https://www.lifewire.com/how-to-test-a-suspicious-link-without-clicking-it-2487171** | accessed on 26 June 2022
[141] Online article | Lifewire | "How to Test a Suspicious Link Without Clicking It" | 2 May 2022 | **https://www.lifewire.com/how-to-test-a-suspicious-link-without-clicking-it-2487171** | accessed on 26 June 2022
[142] Online article | Lifewire | "How to Test a Suspicious Link Without Clicking It" | 2 May 2022 | **https://www.lifewire.com/how-to-test-a-suspicious-link-without-clicking-it-2487171** | accessed on 26 June 2022
[143] E-book | Federal Trade Commission | "Data Brokers: A Call for Transparency and Accountability: A Report of the Federal Trade Commission" | May 2014 **|** **https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014** | accessed on 5 July 2021.
[144] Website | Vice.com | "Here's a Long List of Data Broker Sites and How to Opt-Out of Them" | 27 March 2018 | **https://www.vice.com/en_us/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pipl-spokeo**| accessed on 28 June 2021.
[145] Online article | Motherboard | "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?" | 27 March 2018 **|** **https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection**| accessed on 28 June 2021.
[146] Online article | Fast Company | "Here are the Data Brokers Quietly Buying and Selling your Personal Information" | 2 March 2019 | **https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information**| accessed on 28 June 2021.
[147] Online article | ProPublica | "How to Wrestle Your Data from Data Brokers, Silicon Valley — and Cambridge Analytica" | 30 April 2018 **|** **https://www.propublica.org/article/how-to-wrestle-your-data-from-data-brokers-silicon-valley-and-cambridge-analytica** | accessed on 28 June 2021.
[148] Online article | Quartz | "The Nine Companies That Know More About You Than Google or Facebook" | 27 May 2014 | **https://qz.com/213900/the-nine-companies-that-know-more-about-you-than-google-or-facebook/**| accessed on 28 June 2021.
[149] Online article | Donald W. Reynolds National Center for Business Journalism | "The Business of Personal Data Brokers and Online Privacy" | 2 August 2018 | **https://businessjournalism.org/2018/08/the-business-of-personal-data-brokers-and-online-privacy/** | accessed on 28 June 2021.
[150] Website | Transparencymarketresearch.com | "Data Broker Market" | **https://www.transparencymarketresearch.com/data-brokers-market.html** | accessed on 5 July 2021.
[151] E-Book | Federal Trade Commission | "Data Brokers: A Call for Transparency and Accountability: A Report of the Federal Trade Commission" | May 2014 | **https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014**| accessed on 5 July 2021.
[152] Online article | Mashable | "How to Keep Yourself Safe in a World of Creepy Websites Filled with Personal Data" | 11 January 2017 | **https://mashable.com/2017/01/11/online-security-family-tree-now/**| accessed on 30 June 2021.
[153] Online article | People | "Here's Why This Website That Lets Anyone Find Your Address, Phone Number and More Is Scaring People" | 12 January 2017 | **https://people.com/tech/this-website-lets-anyone-find-your-address-phone-number-and-more-for-free-heres-how-to-opt-out/**| accessed on 30 June 2021.
[154] Online article | Gizmodo | "When a Stranger Decides to Destroy Your Life" | 26 July 2018 | **https://gizmodo.com/when-a-stranger-decides-to-destroy-your-life-1827546385** | accessed on 30 June 2021.
[155] Online article | Lifehacker | "How to Opt Out of the Most Popular People Search Sites" | 4 March 2021 | **https://lifehacker.com/how-to-opt-out-of-the-most-popular-people-search-sites-1791536533** | accessed on 30 June 2021.
[156] Online article | SecurityWeek | "Google Adds Ways to Keep Personal Info Private in Searches" | 29 April 2022 | **https://www.securityweek.com/google-adds-ways-keep-personal-info-private-searches**
[157]Online Article | Google Support | "Remove select personally identifiable info (PII) or doxxing content from Google Search" | **https://support.google.com/websearch/answer/9673730?hl=en#zippy=%2Cwhat-factors-do-we-consider-in-our-evaluation-of-each-request%2Cwhat-happens-to-the-urls-if-theyre-approved-for-removal%2Cthe-intake-form-has-multiple-options-for-removals-which-option-do-i-choose%2Cwhich-urls-do-i-submit-for-review%2Chow-do-i-find-the-url-of-the-content-i-want-to-report%2Chow-do-i-submit-more-than-one-url-for-review%2Cwhy-do-you-ask-for-screenshots-in-the-form%2Chow-do-i-request-removal-of-content-thats-no-longer-live-on-a-website** | accessed on 10 May 2022
[158] Online article | Microsoft Bing | "Content Removal: Report Broken Links or Outdated Cache Pages" | **https://www.bing.com/webmasters/help/bing-content-removal-tool-cb6c294d** | accessed on 10 May 2022
[159] Online article | Tamoco | "Best Guide To Location Data 2022 – All You Need To Know" | 4 September 2019 | **https://www.tamoco.com/blog/location-data-info-faq-guide/**
[160] Online article | Apple Inc. | "App privacy details on the App Store" | **https://developer.apple.com/app-store/app-privacy-details/** | accessed on 10 May 2022

[161] Online article | Apple Inc. | "Location Services & Privacy" | 15 February 2022 | https://www.apple.com/legal/privacy/data/en/location-services/
[162] Online article | Google | "Policy Center > Privacy, Deception and Device Abuse > User Data" | https://support.google.com/googleplay/android-developer/answer/10144311?hl=en | accessed on 10 May 2022
[163] Online article | Vice | "Inside the Industry That Unmasks People at Scale" | 14 July 2021 | https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii| accessed 22 July 2021.
[164] Online article | Privacy News Online | "Keeping Your Digital Footprint Clean During Quarantine" | 29 April 2020 | https://www.privateinternetaccess.com/blog/keeping-your-digital-footprint-clean-during-quarantine/| accessed on 26 July 2021.
[165] Online article | TechCrunch | "Who Gets to Own Your Digital Identity?" | 22 August 2019 | https://techcrunch.com/2019/08/22/who-gets-to-own-your-digital-identity/ | accessed on 27 July 2021.
[166] Online article | Future of Privacy Forum | "A Closer Look at Location Data: Privacy and Pandemics" | 25 March 2020 | https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics/| accessed on 30 July 2021.
[167] Online article | Naked Security by Sophos | "Woman Stalked by Sandwich Server via Her COVID-19 Contact Tracing Info" | https://nakedsecurity.sophos.com/2020/05/14/woman-stalked-by-sandwich-server-via-her-covid-19-contact-tracing-info/| accessed on 30 July 2021.
[168] Press Release | NSA | "How Mobile Device Users Can Limit Their Location Data Exposure" | 4 August 2020 | https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2298930/how-mobile-device-users-can-limit-their-location-data-exposure/ accessed on 22 June 2022.
[169] Online article | Future of Privacy Forum | "New Infographic Illustrates Key Aspects of Location Data" | 22 May 2020 | https://fpf.org/press-releases/new-infographic-illustrates-key-aspects-of-location-data/| accessed on 30 July 2021.
[170] Blog post | National Cybersecurity Alliance | "How Your Phone Number is Exposed: Tips to Protect Your Online Identity" | 26 October 2020 | https://staysafeonline.org/blog/how-your-phone-number-is-exposed/
[171] Blog post | National Cybersecurity Alliance | "How Your Phone Number is Exposed: Tips to Protect Your Online Identity" | 26 October 2020 | https://staysafeonline.org/blog/how-your-phone-number-is-exposed/
[172] Website | CTIA | "How You Can Stop Unwanted Robocalls" | https://fightingrobocalls.ctia.org/#section-05-resources | accessed on 19 May 2022
[173] Website | AT&T | "Download smart security for your smartphone" | https://www.att.com/security/security-apps/ | accessed on 19 May 2022
[174] Website | Verizon | "Shut Down Spam" | https://www.verizon.com/solutions-and-services/call-filter/ | accessed on 19 May 2022
[175] Website | T-Mobile USA, Inc. | "ScamShield" | https://www.t-mobile.com/customers/scam-shield?INTNAV=tNav:Why:BlockScamCalls | accessed on 19 May 2022
[176] Website | UScellular | "Three ways we can help you stop unwanted calls" | https://www.uscellular.com/support/robocall | accessed on 19 May 2022
[177] Website | Federal Trade Commission | "National Do Not call Registry" | https://www.donotcall.gov/ | accessed on 19 May 2022
[178] Online article | CTIA | "How to Stop Robocalls" | https://www.ctia.org/consumer-resources/how-to-stop-robocalls | accessed on 19 May 2022
[179] Online article | Wonder How To | "Find Identifying Information from a Phone Number Using OSINT Tools" | 7 June 2019 | https://null-byte.wonderhowto.com/how-to/find-identifying-information-from-phone-number-using-osint-tools-0195472/ | accessed on 2 July 2021.
[180] Online article | Gizmodo | "Your Old Phone Number Could Get You Hacked, Researchers Say" | 3 May 2021 | https://gizmodo.com/your-old-phone-number-could-get-you-hacked-researchers-1846813781 | accessed on 2 July 2021.
[181] Online article | Gizmodo | "Your Old Phone Number Could Get You Hacked, Researchers Say" | 3 May 2021 | https://gizmodo.com/your-old-phone-number-could-get-you-hacked-researchers-1846813781 | accessed on 2 August 2021.
[182] Online article | Gizmodo | "Your Old Phone Number Could Get You Hacked, Researchers Say" | 3 May 2021 | https://gizmodo.com/your-old-phone-number-could-get-you-hacked-researchers-1846813781 | accessed on 30 July 2021.
[183] Online article | National Cybersecurity Alliance | How Your Phone Number is Exposed: Tips to Protect Your Online Identity | 26 October 2020 | https://staysafeonline.org/blog/how-your-phone-number-is-exposed/
[184] Online article | Safeguarde | "How to Block Restricted Calls on Android and iPhone" | 2021 | https://safeguarde.com/how-to-block-restricted-calls-on-android-and-iphone/ |accessed on 20 July 2021.
[185] Online article | Apple Inc. | "Block phone numbers, contacts, and emails on your iPhone, iPad, or iPod touch" | 20 September 2021 | https://support.apple.com/en-us/HT201229
[186] Online article | Google Phone app Help | "Block or unblock a phone number" | https://support.google.com/phoneapp/answer/6325463 | accessed on 19 May 2022
[187] Online article | Google Android Help | "Check & update your Android version" | https://support.google.com/android/answer/7680439 | accessed on 19 May 2022
[188] Website | CTIA | "How You Can Stop Unwanted Robocalls" | https://fightingrobocalls.ctia.org/#section-05-resources | accessed on 19 May 2022
[189] Online article | Federal Trade Commission | "How To Recognize and Report Spam Text Messages" | February 2020 | https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

[190] Website | CTIA | "Android Robocall Blocking" | **https://www.ctia.org/consumer-resources/how-to-stop-robocalls/android-robocalls-blocking/** | accessed on 19 May 2022
[191] Website | CTIA | "Blackberry Robocall Blocking" | **https://www.ctia.org/consumer-resources/how-to-stop-robocalls/blackberry-robocall-blocking/** | accessed on 19 May 2022
[192] Website | CTIA | "iOS Robocall Blocking" | **https://www.ctia.org/consumer-resources/how-to-stop-robocalls/ios-robocall-blocking/** | accessed on 19 May 2020
[193] Website | CTIA | "Windows Robocall Blocking" | **https://www.ctia.org/consumer-resources/how-to-stop-robocalls/windows-robocall-blocking/** | accessed on 19 May 2022
[194] Online article | Google Messages Help | "Report spam" | **https://support.google.com/messages/answer/9061432?hl=en** | accessed on 19 May 2022
[195] Online article | Apple, Inc. | "Block phone numbers, contacts, and emails on your iPhone, iPad, or iPod touch" | **https://support.apple.com/en-us/HT201229** | 20 September 2021
[196] Online article | Verizon | "SIM Swapping" | **https://www.verizon.com/about/account-security/sim-swapping** | accessed on 19 May 2022
[197] Online article | Department of Justice | "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public" | 08 February 2022 | **https://www.ic3.gov/Media/Y2022/PSA220208**
[198] Online article | Department of Justice | "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public" | 08 February 2022 | **https://www.ic3.gov/Media/Y2022/PSA220208**
[199] Blog post | messente | "How to Protect Yourself from SIM Hijacking" | July 2021 | **https://messente.com/blog/most-recent/sim-hijacking**
[200] Online article | Department of Justice | "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public" | 08 February 2022 | **https://www.ic3.gov/Media/Y2022/PSA220208**
[201] Online article | Apple, Inc. | "Use a SIM PIN for your iPhone or iPad" | 23 September 2021 | **https://support.apple.com/en-us/HT201529**
[202] Online article | efani | "How to Set Up SIM Card Lock on Android?" | **https://www.efani.com/blog/how-to-set-up-sim-card-lock-on-android** | accessed on 19 May 2022
[203] Online article | BlackCloak, Inc. | "How to Protect Your Phone Number from Being Stolen" | **https://blackcloak.io/how-to-protect-your-phone-number-from-being-stolen/** | accessed on 19 May 2022
[204] Online article | TechCrunch | "Cybersecurity 101: How to protect your cell phone number and why you should care" | 25 December 2018 | **https://techcrunch.com/2018/12/25/cybersecurity-101-guide-protect-phone-number/**
[205] Online article | AT&T | "Manage extra security for your wireless account" | **https://www.att.com/support/article/wireless/KM1051397?gsi=Ks1FJro** | accessed on 19 May 2022
[206] Website | T-Mobile USA, Inc. | "Update your Customer PIN/Passcode" | **https://www.t-mobile.com/support/account/update-your-customer-pinpasscode** | accessed on 19 May 2022
[207] Website | Verizon | "Verizon mobile Account PIN FAQs" | **https://www.verizon.com/support/account-pin-faqs/** | accessed on 19 May 2022
[208] Website | Sprint.com | "Learn more about your account PIN" | **https://www.sprint.com/en/support/solutions/account-and-billing/learn-more-about-your-account-pin.html** | accessed on 19 May 2022
[209] Online article | FTC | "What To Know About Credit Freezes and Fraud Alerts" | May 2021 | **https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts**
[210] Website | Equifax | "Security Freeze" | **https://www.equifax.com/personal/credit-report-services/credit-freeze/** | accessed on 19 May 2022
[211] Website | Experian | "Security Freeze" | **https://www.experian.com/freeze/center.html** | accessed on 19 May 2022
[212] Website | TransUnion | "Credit Freeze" | **https://www.transunion.com/credit-freeze** | accessed on 19 May 2022
[213] Online article | FTC | "What To Know About Credit Freezes and Fraud Alerts" | May 2021 | **https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts**
[214] Website | Equifax Inc. | "Let's get started" | **https://my.equifax.com/consumer-registration/rest/1.0/redirectPartnerTenant?intent=FRAUD_ALERT** | accessed on 19 May 2022
[215] Website | Experian | "Fraud alert" | **https://www.experian.com/fraud/center.html#content-01** | accessed on 19 May 2022
[216] Website | TransUnion | "Fraud Alert" | **https://www.transunion.com/fraud-alerts** | accessed on 19 May 2022
[217] Website | FTC | "Report identity theft and get a recovery plan" | **https://www.identitytheft.gov/** | accessed on 19 May 2022
[218] Online article | FTC | "What To Know About Credit Freezes and Fraud Alerts" | May 2021 | **https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts**
[219] Online article | FTC | "Prescreened Credit and Insurance Offers" | May 2021 | **https://consumer.ftc.gov/articles/prescreened-credit-insurance-offers**
[220] Website | FTC | "Credit Bureau Contacts" | **https://www.identitytheft.gov/#/CreditBureauContacts** | accessed on 20 May 2022
[221] Online article | Social Security Administration | "The SSN Numbering Scheme" | **https://www.ssa.gov/history/ssn/geocard.html** | accessed on 10 May 2022

[222] Online article | The Motley Fool | "Everything You Need to Know About Social Security Benefits" | 02 May 2022 | **https://www.fool.com/retirement/social-security/**
[223] Website | Annual CreditReport.com | **https://www.annualcreditreport.com/index.action** | accessed 10 May 2022
[224] Website | Social Security Administration | "Create your personal Social Security account" | **https://www.ssa.gov/myaccount/** | accessed 10 May 2022
[225] Online Document | Social Security Administration | "How You Can Help Us Protect Your Social Security Number and Keep Your Information Safe" | August 2021 | **https://www.ssa.gov/pubs/EN-05-10220.pdf** | accessed 19 June 2022
[226] Website | E-verify.com | "About E-Verify" | 10 April 2018 | **https://www.e-verify.gov/about-e-verify** | accessed on 5 July 2021.
[227] Website | E-verify.com | "Self-Lock" | 7 May 2020 | **https://www.e-verify.gov/mye-verify/self-lock**| accessed on 5 July 2021.
[228] Website | E-verify.com | "Create an Account/Login" | **https://myeverify.uscis.gov/** | accessed on 10 May 2022
[229] Website | E-verify.com | "Create an Account" | **https://myeverify.uscis.gov/** | accessed on 10 May 2022
[230] Online article| the balance | "How to Remove Old Photos of Your Home for Sale From Websites" | 06 January 2022 | **https://www.thebalance.com/remove-old-home-photos-from-real-estate-websites-4102195**
[231] Online article | NSA | "NSA Issues Guidance on Securing Wireless Devices in Public Settings" | 29 July 2021 | **https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2711968/nsa-issues-guidance-on-securing-wireless-devices-in-public-settings/** | accessed on 25 August 2021.
[232] Cybersecurity Information Sheet | NSA | "Securing Wireless Devices in Public Settings" | July 2021 | **https://media.defense.gov/2021/Jul/29/2002815141/-1/-1/0/CSI_SECURING_WIRELESS_DEVICES_IN_PUBLIC.PDF** | accessed on 25 August 2021.
[233] Online article | Norton | "The Dangers of Public Wi-Fi" | 26 May 2018 | **https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html** | accessed on 25 August 2021.
[234] Online article | AT&T Business | "WPA Security Explained: What is Wi-Fi Protected Access?" | 29 June 2020 | **https://cybersecurity.att.com/blogs/security-essentials/wpa-security-explained-what-is-wi-fi-protected-access** | accessed on 23 July 2021.
[235] Online article | PixelPrivacy | "The Real Life Dangers of Using Public Wi-Fi (and How to Protect Yourself When You Have to Use it)" | 23 May 2021 | **https://pixelprivacy.com/resources/public-wifi-dangers/** | accessed on 2 July 2021.
[236] Online article | Cloudwards | "Dangers of Public WiFi: What You Need to Know in 2021" | 8 June 2021 | **https://www.cloudwards.net/dangers-of-public-wifi/** | accessed on 25 August 2021.
[237] Online article | Norton | "The dos and don'ts of using public Wi-Fi" | 23 July 2018 | **https://us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html** | accessed on 25 August 2021.
[238] Online publication | National Security Agency | Keeping Safe on Social Media | August 2021 Ver 1.1 | **https://media.defense.gov/2021/Sep/16/2002855950/-1/-1/0/CSI_KEEPING_SAFE_ON_SOCIAL_MEDIA_20210806.PDF**
[239] Online article | FCC | "Wireless Connections and Bluetooth Security Tips" | 27 July 2021 | **https://www.fcc.gov/consumers/guides/how-protect-yourself-online**
[240] Online article | PixelPrivacy | "Recap: The Best Ways to Protect Your Public Wi-Fi Connection" | 23 July 2021 | **https://pixelprivacy.com/resources/public-wifi-dangers/#Recap_The_Best_Ways_to_Protect_Your_Public_Wi-Fi_Connection** | accessed on 24 July 2021.
[241] Online article | FCC | "Wireless Connections and Bluetooth Security Tips" | 27 July 2021 | **https://www.fcc.gov/consumers/guides/how-protect-yourself-online**
[242] Online article | Department of Justice | "Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide" | 25 May 2018 | **https://www.ic3.gov/Media/Y2018/PSA180525**
[243] Online article | Lifewire | "How to Change a Wi-Fi Network Name" | 02 February 2022 | **https://www.lifewire.com/change-wifi-network-name-5206129**
[244] Online article | Lifewire | "How to Change Your Wireless Router's Admin Password" | 12 march 2021 | **https://www.lifewire.com/how-to-change-your-wireless-routers-admin-password-2487652**
[245] Online article | Lifewire | "MAC Address Filtering: What It Is and How It Works" | 04 August 2021 | **https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571**
[246] Online article | Lifewire | "Why Turning off Your Computer Network Can Help Home and Family Safety" | 08 September 2021 | **https://www.lifewire.com/powered-down-computer-network-817723**
[247] Online publication | National Security Agency | "Best Practices for Keeping Your Home Network Secure" | 18 September 2018 | **https://media.defense.gov/2021/Sep/16/2002855922/-1/-1/0/BEST%20PRACTICES%20FOR%20SECURING%20YOUR%20HOME%20NETWORK%20-%20COPY.PDF**
[248] Online publication | National Security Agency | "Best Practices for Keeping Your Home Network Secure" | 18 September 2018 | **https://media.defense.gov/2021/Sep/16/2002855922/-1/-1/0/BEST%20PRACTICES%20FOR%20SECURING%20YOUR%20HOME%20NETWORK%20-%20COPY.PDF**
[249] Online publication | National Security Agency | "Best Practices for Keeping Your Home Network Secure" | 18 September 2018 | **https://media.defense.gov/2021/Sep/16/2002855922/-1/-1/0/BEST%20PRACTICES%20FOR%20SECURING%20YOUR%20HOME%20NETWORK%20-%20COPY.PDF**

[250] Online article | VPN Overview | "Wi-Fi Location Tracking: How Does It Work?" |17 March 2022 | **https://vpnoverview.com/privacy/devices/wi-fi-location-tracking/** | accessed on 26 June 2022
[251] Online Guide | support. Apple Platform Security | "Wi-Fi Privacy" | **https://support.apple.com/guide/security/wi-fi-privacy-secb9cb3140c/web** | accessed 19 June 2022
[252] Online article | Business Insider | "'What is Bluetooth?': A beginner's guide to the wireless technology" | 20 May 2020 | **https://www.businessinsider.com/what-is-bluetooth** | accessed on 25 August 2021.
[253] Website | OneTemp | "Bluetooth Low Energy: A Closer Look" | **https://www.onetemp.com.au/bluetooth-low-energy-a-closer-look** | accessed on 25 August 2021.
[254] Cybersecurity Information Sheet | NSA | "Securing Wireless Devices in Public Settings" | July 2021 | **https://media.defense.gov/2021/Jul/29/2002815141/-1/-1/0/CSI_SECURING_WIRELESS_DEVICES_IN_PUBLIC.PDF** | accessed on 25 August 2021.
[255] Blog post | AT&T Business | "Bluetooth Security Risks Explained" | 11 June 2020 | **https://cybersecurity.att.com/blogs/security-essentials/bluetooth-security-risks-explained** | accessed on 22 July 2021.
[256] Blog post | Bluetooth Blog | "Proximity and RSSI" | 21 September 2015 | **https://www.bluetooth.com/blog/proximity-and-rssi/** | accessed on 23 July 2021.
[257] Online article | Info Security | "From BIAS to Sweyntooth: Eight Bluetooth Threats to Network Security" | 21 December 2020 | **https://www.infosecurity-magazine.com/opinions/bluetooth-threats-network/** | accessed on 2 July 2021.
[258] Online publication | Franco Zappa | "BIAS: Bluetooth Impersonation Attacks" | **https://francozappa.github.io/about-bias/publication/antonioli-20-bias/antonioli-20-bias.pdf**| accessed on 5 July 2021.
[259] Online article | Threat Post | "Bluetooth Bugs Allow Impersonation Attacks on Legions of Devices" | 19 May 2020 | **https://threatpost.com/bluetooth-bugs-impersonation-devices/155886/**
[260] Online article | InformaTech | "Bluetooth Security Weaknesses Pile Up, While Patching Remains Problematic" | 24 September 2020 | **https://www.darkreading.com/endpoint/bluetooth-security-weaknesses-pile-up-while-patching-remains-problematic/d/d-id/1339009**
[261] Website | Armis.com | "Bleedingbit" | **https://www.armis.com/bleedingbit/** | accessed on 26 May 2022
[262] Online article | TechCrunch | "A pair of new Bluetooth security flaws expose wireless access points to attack" | 1 November 2018 | **https://techcrunch.com/2018/11/01/bleedingbit-security-flaws-bluetooth-wireless-networks/**
[263] Website | Armis.com | "BlueBorne" | **https://www.armis.com/blueborne/** | accessed on 26 May 2022
[264] Online article | Threat Post | "Wireless 'BlueBorne' Attacks Target Billions of Bluetooth Devices" | 12 September 2017 | **https://threatpost.com/wireless-blueborne-attacks-target-billions-of-bluetooth-devices/127921/**
[265] Online article | ZDNet | "Two Billion Devices Still Vulnerable to Blueborne Flaws a Year after Discovery" | 13 September 2018 | **https://www.zdnet.com/article/two-billion-devices-still-exposed-after-blueborne-vulnerabilities-reveal/**
[266] Blog post | AT&T Business | "Bluetooth Security Risks Explained" | 11 June 2020 | https://cybersecurity.att.com/blogs/security-essentials/bluetooth-security-risks-explained | accessed on 22 July 2021.
[267] Online article | Forbes | "Consumers Worry That COVID-19 Contact Tracing Data Will Be Used For Other Purposes -Here's Why" | 24 June 2020 | **https://www.forbes.com/sites/soorajshah/2020/06/24/consumers-worry-that-covid-19-contact-tracing-data-will-be-used-for-other-purposesheres-why/?sh=270431831dfc** | accessed on 23 June 2022.
[268] Online article | Threatpost | "Apple's 'Find My' Network Exploited via Bluetooth" | 13 May 2021 | **https://threatpost.com/apple-find-my-exploited-bluetooth/166121/**
[269] Blog post | Trail of Bits | "You could have Invented that Bluetooth Attack" | 1 August 2018 | **https://blog.trailofbits.com/2018/08/01/bluetooth-invalid-curve-points/**
[270] Website | Knobattack.com | "Key Negotiation of Bluetooth Attack: Breaking Bluetooth Security" | **https://knobattack.com/** | accessed on 26 May 2022
[271] Online article | Security Boulevard | "New Bluetooth Vulnerability, KNOB Attack Can Manipulate the Data Transferred Between Two Paired Devices" | 20 August 2019 | **https://securityboulevard.com/2019/08/new-bluetooth-vulnerability-knob-attack-can-manipulate-the-data-transferred-between-two-paired-devices/**
[272] Online article | Vilabin | "Bluetooth Vulnerabilities: Bluetooth Threats to Network Security" | 21 December 2020 | **https://vilabin.com/article/bluetooth-vulnerabilities-bluetooth-threats-network-security/**
[273] Online article | Asset Research Group | "Unleashing Mayhem Over Bluetooth Low Energy" | 14 July 2020 | **https://asset-group.github.io/disclosures/sweyntooth/**
[274] Online article | HealthITSecurity | "FDA Warns Medical Device Bluetooth Security Flaw Could Disrupt Function" | 5 March 2020 | **https://healthitsecurity.com/news/fda-warns-medical-device-bluetooth-security-flaw-could-disrupt-function**
[275] Online article | Malwarebytes Labs | "Bluetooth Beacons: One Free Privacy Debate with Your Next Order" | 30 June 2020 | **https://blog.malwarebytes.com/privacy-2/2020/06/bluetooth-beacons-one-free-privacy-debate-with-your-next-order/**
[276] Blog post | Blennd | "What is Google Beacon: How Google Beacon Project Affects SEO" | 6 September 2018 | **https://blennd.com/what-is-google-beacon-technology-seo/**
[277] Website | Physicalweb.com | "Walk up and use anything" | **https://google.github.io/physical-web/** | accessed on 26 May 2022
[278] Online article | Pew Research Center | "More Americans Using Smartphones for Getting Directions, Streaming TV" | 29 January 2016 | **https://www.pewresearch.org/fact-tank/2016/01/29/us-smartphone-use/**

[279] Online article | Google | “Helping Public Health Officials Combat COVID-19" | 3 April 2020 | **https://www.blog.google/technology/health/covid-19-community-mobility-reports/**
[280] Online article | Reuters | “In Coronavirus Fight, Oft-Criticized Facebook Data Aids U.S. Cities, States” | 2 April 2020 | **https://www.reuters.com/article/health-coronavirus-facebook-location/in-coronavirus-fight-oft-criticized-facebook-data-aids-u-s-cities-states-idUSKBN21K3BJ**
[281] Blog post | Google: The Keyword | “Helping Public Health Officials Combat COVID-19" | 3 April 2020 | **https://www.blog.google/technology/health/covid-19-community-mobility-reports/**
[282] Website | Nearfieldcommunication.org | “How NFC Works” | 2017 | **http://nearfieldcommunication.org/how-it-works.html** | accessed on 26 May 2022
[283] Website | Nearfieldcommunication.org | “Security Concerns with NFC Technology” | 2017 | **http://nearfieldcommunication.org/nfc-security.html** | accessed on 26 May 2022
[284] Online article | Help Net Security | “Protect Your Smartphone from Radio-Based Attacks” | 19 July 2021 | **https://www.helpnetsecurity.com/2021/07/19/smartphone-radio-based-attacks/**
[285] Website | Century Link | “Understand MAC randomization and Secure WiFi” | **https://www.centurylink.com/home/help/internet/secure-wifi/What-is-MAC-randomization.html** | accessed 19 June 2022
[286] Online Article | Extreme | “What is Wi-Fi MAC Randomization and How Does it Handle Privacy?” | April 30, 2021 | **https://www.extremenetworks.com/extreme-networks-blog/wi-fi-mac-randomization-privacy-and-collateral-damage/** | accessed 19 June 2022
[287] Website | Apple | “Use private Wi-Fi addresses on iPhone, iPad, iPod touch, and Apple Watch” | November 21, 2021 | **https://support.apple.com/en-us/HT211227 |** accessed 19 June 2022
[288] Online Document | Android Open-Source Project | “Wi-Fi Aware” |June 6, 2022 | **https://source.android.com/devices/tech/connect/wifi-aware** | accessed 19 June 2022
[289] Online Document | Android Open-Source Project | “Wi-Fi RTT (IEEE 802.11MC)” | June 6, 2022 | https://source.android.com/devices/tech/connect/wifi-rtt | accessed 19 June 2022
[290] Online Document | Smart-Sources | “About Mobile Location Analytics Technology” | **https://smart-places.org/mobile-location-analytics-opt-out/about-mobile-location-analytics-technology/#beacon** | accessed 19 June 2022
[291] Website | Cliqz | “Google uses credit-card data to track” | **https://cliqz.com/en/magazine/google-uses-credit-card-data-track-offline-purchases** | accessed 19 June 2022
[292] Online Article | Fast Company | “Credit card companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism” | May 12, 2020 | **https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism** | accessed 19 June 2022
[293] Online article | ThreatPost | “6 Questions Attackers Ask Before Choosing an Asset to Exploit” | 29 December 2020 | **https://threatpost.com/6-questions-attackers-ask-exploit/162651/ | accessed on 30 July 2021.**
[294] Online article | ReputationX | “What is a digital footprint?” | 5 June 2022 | https://blog.reputationx.com/digital-footprint | accessed on 23 June 2022
[295] Blog post | Oicon | “Info Exposed: Social Media–The Enemy in Your Home?” | 30 March 2021 | **https://www.osmosiscon.com/info-exposed-social-media-the-enemy-in-your-home/** | accessed on 23 June 2022.
[296] Online article | “Is Your Social Media Activity Leaving You Open to Cyber Attacks?” | 31 August 2020 | **https://socialmediaexplorer.com/content-sections/tools-and-tips/is-your-social-media-activity-leaving-you-open-to-cyber-attacks/**
[297] Online article | Experian | “How to Manage Your Privacy Settings on Social Media” | 30 March 2018 | **https://www.experian.com/blogs/ask-experian/how-to-manage-your-privacy-settings-on-social-media/**
298 Online publication | The Wall Street Journal | “What Hackers Can Learn About You From Your Social-Media Profile” | 8 June 2021 | https://www-wsj-com.cdn.ampproject.org/c/s/www.wsj.com/amp/articles/what-hackers-can-learn-about-you-from-your-social-media-profile-11623157200
[299] Online publication | National Security Agency | Keeping Safe on Social Media | August 2021 Ver 1.1 | **https://media.defense.gov/2021/Sep/16/2002855950/-1/-1/0/CSI_KEEPING_SAFE_ON_SOCIAL_MEDIA_20210806.PDF**
[300] Online publication | National Security Agency | Keeping Safe on Social Media | August 2021 Ver 1.1 | **https://media.defense.gov/2021/Sep/16/2002855950/-1/-1/0/CSI_KEEPING_SAFE_ON_SOCIAL_MEDIA_20210806.PDF**
[301] Online Article | Discord | “Discord Community Guidelines” | **https://discord.com/guidelines** | accessed 22 June 2022
[302] Online Article | Discord | “Moderating on Discord” | **https://discord.com/moderation** | accessed 22 June 2022
[303] Online Article | Discord | “Setting up Two-Factor Authentication” | **https://support.discord.com/hc/en-us/articles/219576828-Setting-up-Two-Factor-Authentication** | accessed 22 June 2022
[304] Online Article | Discord | “Submit a request” | **https://support.discord.com/hc/en-us/requests/new?ticket_form_id=360000029731** | accessed 22 June 2022
[305] Online Article | Kaspersky | “Guide to Twitch: Twitch safety and security” | **https://usa.kaspersky.com/resource-center/preemptive-safety/guide-to-twitch-safety-and-security** | accessed 19 June 2022
[306] Online Article | Technipages | “Twitch.tv: How to Manage Your Privacy Settings” | **https://www.technipages.com/twitch-tv-manage-privacy-settings** | accessed 19 June 2022

[307] Online Article | Twitch |"How to Manage Harassment in Chat" | **https://help.twitch.tv/s/article/how-to-manage-harassment-in-chat?language=en_US** | accessed 22 June 2022
[308] Online Article | Twitch |"How to Manage Harassment in Chat" | **https://help.twitch.tv/s/article/how-to-manage-harassment-in-chat?language=en_US** | accessed 22 June 2022
[309] Online Article | Twitch | "Your Privacy Choices" | **https://www.twitch.tv/p/en/legal/privacy-choices/** | accessed 22 June 2022
[310] Online article | Lifewire | "What is Facebook?" | 19 September 2021 | **https://www.lifewire.com/what-is-facebook-3486391**
[311] Online article | Social Media Today | "Facebook Outlines Its Ad Review Process to Provide More Transparency on Its System" | 20 May 2021 | **https://www.socialmediatoday.com/news/facebook-outlines-its-ad-review-process-to-provide-more-transparency-on-its/600580/**
[312] Website | Meta | "How Ads Work on Facebook" | **https://www.facebook.com/help/516147308587266/how-ads-work-on-facebook/?helpref=hc_fnav** | accessed on 26 May 2022
[313] Online article | Meta | How can I make my Facebook password strong? | **https://www.facebook.com/help/124904560921566** | accessed on 11 May 2022
[314] Online article | security.org | How Secure Is My Password? | **https://www.security.org/how-secure-is-my-password/** | accessed on 11 May 2022
[315] Online article | Meta | How do I get alerts about unrecognized logins to Facebook? | **https://www.facebook.com/help/162968940433354** | accessed on 11 May 2022
[316] Online article | Meta | What is two-factor authentication and how does it work on Facebook? | **https://www.facebook.com/help/148233965247823** | accessed on 11 May 2022
[317] Online article | Meta | How can I choose friends to help me log in if I ever get locked out of my Facebook account? | **https://www.facebook.com/help/119897751441086** | accessed on 11 May 2022
[318] Online article | Social Media Today | "Facebook Outlines New Differential Privacy Framework to Protect User Information in Shared Datasets" | 3 June 2020 | **https://www.socialmediatoday.com/news/facebook-outlines-new-differential-privacy-framework-to-protect-user-inform/579167/**
[319] Online article | Meta | How do I log out of Facebook on another computer, phone, or tablet? | **https://www.facebook.com/help/211990645501187** | accessed on 11 May 2022
[320] Online article | Meta | How do I choose what I get notifications about on Facebook? | **https://www.facebook.com/help/390022341057202** | accessed on 11 May 2022
[321] Online article | Meta | What's Facebook Security Checkup and how do I start it? | **https://www.facebook.com/help/799880743466869** | accessed on 11 May 2022
[322] Online article | How-to Geek | "7 Important Facebook Privacy Settings to Change Right Now" | 2 June 2021 | **https://www.howtogeek.com/727135/7-important-facebook-privacy-settings-to-change-right-now/**
[323] Online article | Forbes | "Facebook Cites Russia and Iran as Its Top Sources Of Disinformation [Infographic]" | 27 May 2021 | **https://www.forbes.com/sites/niallmccarthy/2021/05/27/facebook-cites-russia-and-iran-as-its-top-sources-of-disinformation-infographic/**
[324] Online article | Meta | When I post something on Facebook, how do I choose who can see it? | **https://www.facebook.com/help/120939471321735** | accessed on 11 May 2022
[325] Online article | How-toGeek | "6 Things You Should Never Share on Facebook and Social Media" |15 May 2021 | **https://www.howtogeek.com/723834/6-things-you-should-never-share-on-facebook-and-social-media/**
[326] Online article | Meta | How do I review tags that people add to my Facebook posts before they appear? | **https://www.facebook.com/help/247746261926036** | accessed on 11 May 2022
[327] Website | Meta | Control Who Can Find You | **https://www.facebook.com/help/392235220834308** | accessed on 11 May 2022
[328] Online article | Forbes | "All The Ways Facebook Tracks You And How To Stop It" | 8 May 2021 | **https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/kateoflahertyuk/2021/05/08/all-the-ways-facebook-tracks-you-and-how-to-stop-it/amp/**
[329] Online article | Forbes | All The Ways Facebook Tracks You And How To Stop It" | 8 May 2021 | **https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/kateoflahertyuk/2021/05/08/all-the-ways-facebook-tracks-you-and-how-to-stop-it/amp/**
[330] Online article | Meta | Location privacy | **https://www.facebook.com/help/477587325603876** | accessed 24 May 2022.
[331] Online article | Meta | How can I see what my profile looks like to people on Facebook I'm not friends with? | **https://www.facebook.com/help/288066747875915** | accessed 12 May 2022
[332] Website | Meta | Facebook Ad Preferences | **https://www.facebook.com/help/109378269482053/?helpref=hc_fnav** | accessed on 12 May 2022
[333] Online article | HackRead | "Facebook Exposed User Data to Thousands of App Developers" | 2 July 2020 | **https://www.hackread.com/facebook-exposed-user-data-to-app-developers/**
[334] Website | Meta | "What is the face recognition setting on Facebook and how does it work?" Facebook Help | **https://www.facebook.com/help/122175507864081** | accessed on 12 May 2022
[335] Website | Meta | "Adding Friends" Facebook Help | **https://www.facebook.com/help/246750422356731/?helpref=hc_fnav** | accessed on 12 May 2022

[336] Website | Meta | "Unfriending or Blocking Someone" Facebook Help | **https://www.facebook.com/help/301707886595168** | accessed on 12 May 2022
[337] Online article | How-to Geek | "How to Restrict Someone on Facebook" | 29 May 2021 | **https://www.howtogeek.com/728204/how-to-restrict-someone-on-facebook/**
[338] Online Article | Meta | "What is blocking on Facebook and how do I block someone?" | **https://www.facebook.com/help/168009843260943?_rdc=1&_rdr=** | accessed on 12 May 2022
[339] Online article | Meta | What happens when I report something to Facebook? Does the person I report get notified? | **https://www.facebook.com/help/103796063044734** | accessed on 12 May 2022
[340] Online article | Webopedia | https://www.webopedia.com/definitions/facebook-messenger/| accessed on 4 October 2021
[341] Website | Meta | "How do I upload my contacts to Messenger?" Facebook help | **https://www.facebook.com/help/messenger-app/838237596230667** | accessed on 12 May 2022
[342] Online article | Meta | "What is Active Status and how does it work?" Facebook Messenger Help | **https://www.facebook.com/help/messenger-app/321774648351848** | accessed 12 May 2022
[343] Online article | Meta | "How do I control who can send a message to my Messenger Chats list?" Facebook Messenger Help | **https://www.facebook.com/help/messenger-app/2258699540867663** | accessed on 12 May 2022
[344] Website | Meta | "Secret Conversations" Facebook Messenger Help | **https://www.facebook.com/help/messenger-app/1084673321594605** | accessed on 12 May 2022
[345] Website | Meta | "How do I clear my Search History in Messenger?" Facebook Messenger Help | **https://www.facebook.com/help/messenger-app/362238567897910** | accessed on 12 May 2022
[346] Online article | Meta | "How do I remove or unsend a message that I've sent in Messenger?" Facebook Messenger Help | **https://www.facebook.com/help/messenger-app/194400311449172** | accessed on 12 May 2022
[347] Website | Meta | "How do I choose who can see my story from the Messenger app?" Facebook Messenger Help | **https://www.facebook.com/help/messenger-app/146668145777564** | accessed on 12 May 2022
[348] Online article | Makeuseof.com | "What Is Instagram and How Does It Work?" | 09 July 2021 | **https://www.makeuseof.com/tag/what-is-instagram-how-does-instagram-work/**
[349] Online article | Instagram Community Guidelines | "Community Guidelines" | **https://help.instagram.com/477434105621119** | accessed on 27 June 2022
[350] Online article | Instagram Help Center | "Privacy Settings & Information" | **https://help.instagram.com/196883487377501/?helpref=hc_fnav** | accessed on 27 June 2022
[351] Online article | Wired | "How to Stop Instagram from Tracking Everything You Do" | 6 June 2020 | **https://www.wired.co.uk/article/instagram-story-ads-privacy-delete**
[352] Online article | How-to Geek | "How to Turn off Message Requests in Instagram" | 2 May 2021 | **https://www.howtogeek.com/721386/how-to-turn-off-message-requests-in-instagram/**
[353] Online article | Meta | "How Can I Adjust How Ads on Instagram are Shown to me Based on Data About my Activity from Partners?" | **https://www.facebook.com/help/instagram/2885653514995517?helpref=faq_content**
[354] Online article | Instagram Help Center | "How do I clear my Instagram search history?" | **https://help.instagram.com/354860134605952** | accessed on 27 June 2022
[355] Online article | Instagram Help Center | "Sharing Photos Safely" | **https://help.instagram.com/646840095358740/?helpref=hc_fnav** | accessed on 27 June 2022
[356] Website | Meta | "Data Policy" Instagram | **https://help.instagram.com/519522125107875/?maybe_redirect_pol=0** | accessed on 12 May 2022
[357] Online article | Instagram Help Center | "How do I disconnect my Instagram account from another social network?" | **https://help.instagram.com/536741816349927** | accessed on 27 June 2022
[358] Website | Instagram for Parents | "Helping your teen navigate Instagram safely "| **https://about.instagram.com/community/parents** | accessed on 19 June 2022
[359] Online article | LinkedIn Help | "What is LinkedIn and How Can I Use It?" | March 2022 | **https://www.linkedin.com/help/linkedin/answer/111663/what-is-linkedin-and-how-can-i-use-it-?lang=en**
[360] Online Article | Secureworks | "Social Engineering Tactics: Why LinkedIn is a Dangerous as it is Useful" | March 3, 2022 | **https://www.secureworks.com/blog/social-engineering-tactics-why-linkedin-is-as-dangerous-as-it-is-useful** | accessed 19 June 2022
361 Online article | Security Intelligence | "Social Engineering: How to Keep Security Researchers Safe" | 16 May 2021 | **https://securityintelligence.com/articles/social-engineering-keep-security-researchers-safe/**
[362] Online article | Department of Justice | "Cyber Criminals Use Fake Job Listings To Target Applicants' Personally Identifiable Information" | 21 January 2020 | **https://www.ic3.gov/Media/Y2020/PSA200121**
[363] Online article | Department of Justice | "Cyber Criminals Use Fake Job Listings To Target Applicants' Personally Identifiable Information" | 21 January 2020 | **https://www.ic3.gov/Media/Y2020/PSA200121**
[364] Website | Google | Google Translate | **https://translate.google.com/intl/en/about/** | accessed on 12 May 2022
[365] Online article | LinkedIn Corp | "Understanding Your Privacy Settings" | 27 August 2020 | **https://www.linkedin.com/help/linkedin/answer/92055/understanding-your-privacy-settings?lang=en**

[366] Online article | LinkedIn Corp | "Managing Your Account and Privacy Settings - Overview" | 3 September 2020 | https://www.linkedin.com/help/linkedin/answer/66
[367] Online article | LinkedIn Corp | "Similarities and Differences Between Following and Connecting" | 22 April 2022 | https://www.linkedin.com/help/linkedin/answer/a527006/similarities-and-differences-between-following-and-connecting?lang=en
[368] Online article | LinkedIn Corp | "View Your Followers" | 26 April 2022 | https://www.linkedin.com/help/linkedin/answer/a541884
[369] Online article | LinkedIn Corp | "Manage Who Can Follow Your Updates" | 12 December 2021 | https://www.linkedin.com/help/linkedin/answer/a528011
[370] Online article | CQCore | "Are You Linked In?" | 24 May 2021 | https://www.cqcore.uk/are-you-linked-in/
[371] Online article | LinkedIn Corp | "Search for People on LinkedIn" | 12 April 20022 | https://www.linkedin.com/help/linkedin/answer/a525054
[372] Online article | LinkedIn Corp | "Using Boolean Search on LinkedIn" | 12 December 2021 | https://www.linkedin.com/help/linkedin/answer/a524335/using-boolean-search-on-linkedin?lang=en
[373] Online article | LinkedIn Corp | "Your Network and Degrees of Connection" | 12 March 2022 | https://www.linkedin.com/help/linkedin/answer/a545636/your-network-and-degrees-of-connection?lang=en
[374] Website | Support.snapchat.com | "Snapchat Support" | https://support.snapchat.com/en-US |accessed on 9 August 2021
[375] Online article | Common Sense Media | "Parents' Ultimate Guide to Snapchat" | 9 March 2021 | https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-snapchat
[376] Website | Snap Inc. | "Control Over Your Information" | https://snap.com/en-US/privacy/privacy-policy/#control-over-your-information | accessed on 24 May 2022
[377] Blog post | Privacycrypts | "Snapchat Privacy Settings And Tips In 2022" | 01 January 2022 | https://privacycrypts.com/blog/snapchat-privacy-settings-tips/
[378] Website | Snap Inc. | "How We Use Your Information" | https://snap.com/en-US/privacy/your-information | accessed on 24 May 2022
[379] Online article | Influencer Marketing Hub | "What is TikTok? – Everything You need to know in 2022" | 31 March 2022 | https://influencermarketinghub.com/what-is-tiktok/
[380] Online article | Personal Privacy Solutions Ltd. | "Privacy on TikTok: How to protect you and your family" | 12 August 2020 | https://tapmydata.com/privacy-on-tiktok-how-to-protect-you-and-your-family/
[381] Online article | 9TO5Mac | "TikTok Privacy Policy Now Says App Will Collect 'Faceprints and Voiceprints'" | 4 June 2021 | https://9to5mac.com/2021/06/04/tiktok-privacy-policy-now-says-app-will-collect-faceprints-and-voiceprints/
[382] Online article | Lifewire | "What Is Twitter & How Does It Work?" | 29 August 2021 | https://www.lifewire.com/what-exactly-is-twitter-2483331
[383] Online article | Twitter Help Center | "New user FAQ" | https://help.twitter.com/en/resources/new-user-faq | accessed on 24 May 2022
[384] Website | Twitter Help Center | "What Can we Help you Find?" | https://help.twitter.com/ | accessed on 24 May 2022
[385] Online article | Twitter Help Center | "Following FAQs" | https://help.twitter.com/en/using-twitter/following-faqs.html | accessed on 24 May 2022
[386] Online article | Twitter Help Center | "How to Control your Twitter Experience" | https://help.twitter.com/en/safety-and-security/control-your-twitter-experience | accessed on 24 May 2022
[387] Online article | Twitter Help Center | "How to Protect your Personal Information" | https://help.twitter.com/en/safety-and-security/twitter-privacy-settings | accessed on 24 May 2022
[388] Online article | Malwarebytes Labs | "Have I Been Pwnd?"– What Is It and What To Do When You *Are* Pwned" | 20 May 2021 | https://blog.malwarebytes.com/awareness/2021/05/have-i-been-pwnd-what-is-it-and-what-to-do-when-you-are-pwned/
[389] Online article | Twitter Help Center | "How to Protect your Personal Information" | https://help.twitter.com/en/safety-and-security/twitter-privacy-settings | accessed on 24 May 2022
[390] Online article | Twitter Help Center | "How to protect your personal information" https://help.twitter.com/en/safety-and-security/twitter-privacy-settings | accessed on 12 May 2022
[391] Online article | Defending Digital | "Don't Share Your Birth Date Online – Best Digital Privacy Tips In 2022" | https://defendingdigital.com/dont-share-your-birth-date-online/ | accessed on 12 May 2022
[392] Online article | Twitter Help Center | "How to Protect and Unprotect your Tweets" | https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public | accessed on 24 May 2022
[393] Online Article | Twitter | "Safety and Security" | https://help.twitter.com/en/safety-and-security | accessed 22 June 2022
[394] Online article | Twitter Help Center | "About Account Security" | https://help.twitter.com/en/safety-and-security/account-security-tips | accessed on 24 May 2022
[395] Online Article | Twitter Help Center | "How to use precise location on mobile devices" | https://help.twitter.com/en/safety-and-security/twitter-location-services-for-mobile | accessed on 12 May 2022
[396] Website | Support.google.com | "Understanding the Basics of Privacy on YouTube Apps" | 2021 | https://support.google.com/youtube/answer/10364219?hl=en | accessed on 22 June 2022
[397] Online article | Twitter Help Center | "How to mute accounts on Twitter" | https://help.twitter.com/en/using-twitter/twitter-mute | accessed on 12 May 2022

[398] Online article | Twitter Help Center | "How to use two-factor authentication" | **https://help.twitter.com/en/managing-your-account/two-factor-authentication** | accessed on 24 May 2022
[399] Online article | Bitdefender | "Despite All the Advice, 97.7% of Twitter Users Have Still Not Enabled Two-Factor Authentication" | 27 July 2021 | **https://www.bitdefender.com/blog/hotforsecurity/despite-all-the-advice-97-7-of-twitter-users-have-still-not-enabled-two-factor-authentication** | accessed on 24 May 2022
[400] Online article | Defending Digital | "Twitter Security And Privacy Guide 2022" | **https://defendingdigital.com/twitter-security-privacy-guide/** | accessed on 12 May 2022
[401] Online article | Lifewire | "What Is YouTube: A Beginner's Guide" | 02 December 2020 | **https://www.lifewire.com/youtube-101-3481847** | accessed on 24 May 2022
[402] Website | YouTube Help | "Change your Subscription Privacy Settings" | **https://support.google.com/youtube/answer/7280190?hl=en&ref_topic=9257519** | accessed on 24 May 2022
[403] Website | Youtube.com | "Privacy Controls" | **https://www.youtube.com/howyoutubeworks/user-settings/privacy/** | accessed on 24 May 2022
[404] Website | Support.google.com | "Understanding the Basics of Privacy on YouTube Apps" | 2021 | **https://support.google.com/youtube/answer/10364219?hl=en** | accessed on 22 June 2022
[405] Website | Support.google.com | "Update your Location Settings in YouTube Music" | **https://support.google.com/youtubemusic/answer/9015821** | accessed on 24 May 2022
[406] Online article | YouTube Help | "View, clear, or pause watch history (signed in)" | **https://support.google.com/youtube/answer/95725** | accessed on 12 May 2022
[407] Website | Support.google.com | "Watching 'Made for Kids' Content" | 2021 | **https://support.google.com/youtube/answer/9632097**
[408] Online article | Google Account Help | "Age requirements on Google Accounts" | **https://support.google.com/accounts/answer/1350409** | accessed on 12 May 2022
[409] Online article | AndroidCentral | "How to Set Up Supervised Accounts for your Kids on YouTube" | 8 May 2021 | **https://www.androidcentral.com/how-set-supervised-accounts-your-kids-youtube**
[410] Website | Google | Help your family create healthy digital habits | **https://families.google.com/familylink/** | accessed on 12 May 2022
[411] Online article | Techopedia | "What is Google – Definition from Techopedia" | 13 May 2020 | **https://www.techopedia.com/definition/5359/google**
[412] Online article | Axios | "What Google Knows About You" | 11 March 2019 | **https://www.axios.com/what-google-knows-about-you-3f6c9b20-4406-4bda-8344-d324f1ee0816.html**
[413] Online article | Lifehacker | "How to Limit Google's Apps From Tracking You on Your Apple Devices" | 25 February 2021 | **https://lifehacker.com/how-to-limit-googles-apps-from-tracking-you-on-your-app-1846357454** | accessed on 11 August 2021
[414] Online article | Visual Capitalist | "What Does Google Know About You?" | 10 August 2018 | **https://www.visualcapitalist.com/what-does-google-know-about-you/**
[415] Online article | Wired | "All the Ways Google Tracks You—And How to Stop It" | 27 May 2019 | **https://www.wired.com/story/google-tracks-you-privacy/**
[416] Website | Google Privacy Controls | "Privacy tools that put you in control" | **https://safety.google/privacy/privacy-controls/** | accessed on 12 May 2022
[417] ZDNet | ZDNet | "Google revamps privacy policy to give users more control over Assistant voice recordings" | 23 September 2019 | **https://www.zdnet.com/article/google-revamps-privacy-policy-to-give-users-more-control-over-assistant-voice-recordings/**
[418] Blog post | Google: The Keyword | "Doing More to Protect your Privacy with the Assistant" | 23 September 2019 | **https://www.blog.google/products/assistant/doing-more-protect-your-privacy-assistant/**
[419] Online article | Forbes | "Google to Fix Malicious Invites Issue for 1 Billion Calendar Users" | 9 September 2019 | **https://www.forbes.com/sites/daveywinder/2019/09/09/google-finally-confirms-security-problem-for-15-billion-gmail-and-calendar-users/#e7f62c3279fa**
[420] Online article | Black Hills Information Security | "Google Calendar Event Injection with MailSniper" | 1 November 2017 | **https://blackhillsinfosec.com/google-calendar-event-injection-mailsniper/**
[421] Online article | Fast Company | "Amazon: Most Innovative Company" | **https://www.fastcompany.com/company/amazon** | accessed on 23 May 2022
[422] Website | Amazon | "How Amazon Collects Your Personal Information" | **https://www.amazon.com/gp/help/customer/display.html/?nodeId=GSXETHUPY4UM7CRD** | accessed on 23 May 2022
[423] Website | Amazon | "How Amazon Uses Your Personal Information" | **https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=G6CVQVUVGMD3BJQ2** | accessed on 23 May 2022
[424] Website | Amazon | "Interest-Based Ads" | **https://www.amazon.com/gp/help/customer/display.html/?nodeId=GLVB9XDF9M8MU7UZ** | accessed on 23 May 2022
[425] Website | Amazon | "Amazon.com Privacy Notice" | 12 February 2021 | **https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ** | accessed on 23 May 2022

[426] Online article | Wired | "All the Ways Amazon Tracks You—and How to Stop It" | 22 June 2021 | https://www.wired.com/story/amazon-tracking-how-to-stop-it/
[427] Online article | The Hacker News | "Your Amazon Devices to Automatically Share Your Wi-Fi With Neighbors" | 31 May 2021 | https://thehackernews.com/2021/05/your-amazon-devices-to-automatically.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29 | accessed on 23 May 2022
[428] Website | Amazon Help & Customer Service | "Saving Your Wi-Fi Passwords to Amazon FAQs" |https://www.amazon.com/gp/help/customer/display.html?nodeId=201730860 | accessed on 19 June 2022
[429] Website | Amazon Help & Customer Service | "Saving Your Wi-Fi Passwords to Amazon FAQs" |https://www.amazon.com/gp/help/customer/display.html?nodeId=201730860 | accessed on 19 June 2022
[430] Website | Amazon Help & Customer Service | "Saving Your Wi-Fi Passwords to Amazon FAQs" |https://www.amazon.com/gp/help/customer/display.html?nodeId=201730860 | accessed on 19 June 2022
[431] Website | Amazon.com, Inc. | Password Assistance | https://www.amazon.com/ap/forgotpassword?openid.pape.max_auth_age=900&openid.assoc_handle=usflex&openid.mode=checkid_setup&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0 | accessed on 12 May 2022
[432] Website | Amazon | "About Security Alerts" | https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=GLXNK37D6R3WGXKW | accessed on 23 May 2022
[433] Online article | Amazon.com Help & Customer Service | "Two-Step Verification" | https://www.amazon.com/gp/help/customer/display.html?nodeId=201596330 | accessed on 12 May 2022
[434] Online article | Amazon.com Help & Customer Service | "Resolve Common Two-Step Verification Issues" | https://www.amazon.com/gp/help/customer/display.html?nodeId=201962400 | accessed on 12 May 2022
[435] Online article | Technastic Media | "How to Enable Two-Step Verification on the Amazon app" | 29 March 2020 | https://technastic.com/two-step-verification-amazon/
[436] Online article | Amazon.com Help & Customer Service | "About Multi-Factor Authentication" | https://www.amazon.com/gp/help/customer/display.html?nodeId=G9MX9LXNWXFKMJYU | accessed on 12 May 2022
[437] Online article | Amazon.com Help & Customer Service | "Secure Delivery with a One-Time Password" | https://www.amazon.in/gp/help/customer/display.html?nodeId=202122140 | accessed on 12 May 2022
[438] Online article | Amazon.com Help & Customer Service | "Change Your Purchase Settings" | https://www.amazon.com/gp/help/customer/display.html?nodeId=201889370 | accessed on 12 May 2022
[439] Online article | Amazon.com Help & Customer Service | "Change Your Purchase Settings" | https://www.amazon.com/gp/help/customer/display.html?nodeId=201889370 | accessed on 12 May 2022
[440] Online article | Amazon.com Help & Customer Service | "Update Your Mobile Buy Now Settings" | https://www.amazon.com/gp/help/customer/display.html?nodeId=201889170 | accessed on 12 May 2022
[441] Online article | Amazon.com Help & Customer Service | "Ask Alexa to Delete Your Voice History" | https://www.amazon.com/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=GYRPHMGANH7M2BNH | accessed on 19 May 2022
[442] Online article | Amazon.com Help & Customer Service | "Ask Alexa to Delete Your Voice History" | https://www.amazon.com/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=GYRPHMGANH7M2BNH | accessed on 19 May 2022
[443] Website | Amazon Help and Customer Service | "Alexa and Alexa Device FAQs" | https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 | accessed 19 June 2022
[444] Online article | Amazon.com Help & Customer Service | "Ask Alexa to Delete Your Voice History" | https://www.amazon.com/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=GYRPHMGANH7M2BNH | accessed on 19 May 2022
[445] Online article | Amazon.com Help & Customer Service | "Delete Alexa Voice Recordings Automatically" | https://www.amazon.com/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=G68KUKTXN92WY3C3 | accessed on 19 May 2022
[446] Website | Amazon Help and Customer Service | "Turn Alexa Voice Purchasing On or Off" | https://www.amazon.com/gp/help/customer/display.html?nodeId=GPUCQ6PMPMENG8FA | accessed 19 June 2022
[447] Website | Amazon Help and Customer Service | "Manage an Alexa Voice ID for Purchases with Alexa" | https://www.amazon.com/gp/help/customer/display.html?nodeId=GKW8N2S4UQ2SAEBL | accessed 19 June 2022
[448] Website | Amazon Help and Customer Service | "Require a Voice Code for Purchases with Alexa" | https://www.amazon.com/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=GAA2RYUEDNT5ZSNK | accessed 19 June 2022
[449] Online article | CNet | "Amazon's Alexa can now sense the presence of people. Here's how to use the uncanny new trick" | 11 June 2021 | https://www.cnet.com/home/smart-home/amazons-alexa-can-now-sense-the-presence-of-people-heres-how-to-use-the-uncanny-new-trick/ | accessed on 25 June 2022

[450] Online article | Kim Komando | "Amazon Sidewalk: Should you opt-out of the neighborhood wireless network?" | 27 November 2020 | https://www.komando.com/security-privacy/amazon-sidewalk-opt-out/766731/
[451] Online article | AndroidCentral | "What You Need to Know About Amazon Sidewalk Before You Decide to Opt Out" | 26 June 2021 | https://www.androidcentral.com/what-you-need-know-about-amazon-sidewalk-you-decide-opt-out | accessed on 9 August 2021.
[452] Online article | The Verge | "How to Opt Out of (or into) Amazon's Sidewalk Network" | 1 June 2021 | https://www.theverge.com/22463257/amazon-sidewalk-privacy-how-to-opt-out | accessed on 23 May 2022
[453] Online article | Amazon.com Help & Customer Service | "Welcome to Amazon Sidewalk" | https://www.amazon.com/gp/help/customer/display.html?nodeId=GN9U5W9UZU2G5VBW | accessed on 12 May 2022
[454] Website | Amazon Sidewalk | "What are Sidewalk Bridges, and which devices are able to become Sidewalk Bridges?" | https://www.amazon.com/gp/browse.html?node=21328123011&ref%5F=pe%5F41837490%5F547199770%5Fpe%5Fmp%5Ftran%5Faucc%5Fsidewalk%5Flearn&pldnSite=1#:~:text=What%20are%20Sidewalk%20Bridges%2C%20and%20which%20devices%20are%20able%20to%20become%20Sidewalk%20Bridges%3F | accessed on 12 May 2022
[455] Online publication | Amazon.com, Inc. | "Amazon Sidewalk Privacy and Security Whitepaper" | https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf | accessed on 12 may 2022
[456]Website | Amazon Help and Customer Service | "Enable or Disable Amazon Sidewalk for Your Account" | https://www.amazon.com/gp/help/customer/display.html?ref_=hp_gcs_csd_d2_649_3_GZ4VSNFMBDHLRJUK&nodeId=GZ4VSNFMBDHLRJUK&sr=3 | accessed 19 June 2022
[457] Online article | Department of Justice | "Child Predators Use Online Gaming to Contact Children" | 12 December 2019 | https://www.ic3.gov/Media/Y2019/PSA191212
[458] Online article | Wikipedia | "Cord-cutting" | 7 February 2022 | https://en.wikipedia.org/wiki/Cord-cutting
[459]Online article | Insider Intelligence eMarketer | "Connected TV Advertising" | 23 August 2018 | https://www.emarketer.com/content/connected-tv-advertising
[460] Online article | JCH Media Inc. | "One Billion Internet-Connected TV Devices in Use Globally" | 14 August 2018 | https://www.mediaplaynews.com/one-billion-internet-connected-tv-devices-in-use-globally/
[461] Online Article | New York Times | 5 July 2018 | "How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight" | https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html)
[462] Online article | Vox Medic, LLC. | "Smart TVs are data-collecting machines, new study shows" | 11 October 2019 | https://www.theverge.com/2019/10/11/20908128/smart-tv-surveillence-data-collection-home-roku-amazon-fire-princeton-study
[463] Online article | Consumer Reports Inc. | "How to Turn Off Smart TV Snooping Features" | 17 February 2021 | https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/
[464] Online Article | Avast | "What is Ad Tracking?" | https://www.avast.com/c-what-is-ad-tracking | accessed 22 June 2022
[465] Online Article | Avast | "Internet of Things Security Risk" | https://www.avast.com/c-iot-security-risks | accessed 22 June 2022
[466] Online Article | Avast | "How to Protect Yourself Against Router Hacking" | https://www.avast.com/c-prevent-router-hacks | accessed 22 June 2022
[467] Online Article | Choozle, Inc. | "Connected TV (CTV) Inventory Terminology" | 14 April 2020 | https://choozle.com/blog/ctv-inventory/
[468] Website | NAI: Network Advertising Initiative | "Learn About Internet Connected TV Choices" | https://thenai.org/opt-out/connected-tv-choices/ | accessed on 12 May 2022
[469] Website | NAI: Network Advertising Initiative | "Opt Out" | https://thenai.org/opt-out/ | accessed on 12 May 2022
[470] Online article | Consumer Reports| "How to Keep Your Home Security Cameras From Being Hacked" | 4 May 2022 | https://www.consumerreports.org/home-security-cameras/keep-home-security-cameras-from-being-hacked-a2927068390/ | accessed on 27 June 2022
[471] Online article | DigitalTrends | "Which smart security cams are serious about privacy? We've ranked them all" | 24 May 2022 | https://www.digitaltrends.com/home/security-camera-scorecard-feature-comparison/ | accessed on 27 June 2022
[472] Online article | SafeHome.org | "Best Home Security Cameras of 2022" | 24 May 2022 | https://www.safehome.org/home-security-cameras/best/ | accessed on 27 June 2022
[473] Online Article | Mashable | "The best home security cameras for privacy and peace of mind" | August 4, 2021 | https://mashable.com/roundup/best-security-cameras | accessed 19 June 2022
[474] Online Article | Wired | "The Best Indoor Security Cameras" | October 6, 2021 | https://www.wired.com/gallery/best-security-cameras/ | accessed 19 June 2022
[475] Online Article | Digital Trends | "Why privacy shutters on security cameras make all the difference" | April 2, 2021 | https://www.digitaltrends.com/home/why-your-security-cameras-privacy-shutter-matters/ | accessed 19 June 2022
[476] Online Article | AndroidCentral| "Best security cameras with local storage 2022" | June 15, 2022 | https://www.androidcentral.com/best-security-cameras-store-locally-not-cloud | accessed 19 June 2022
[477] Online Article | Safewise | "Best Motion Sensor Security Cameras of 2022" | May 3, 2022 | https://www.safewise.com/resources/best-motion-sensor-cameras/ | accessed 19 June 2022
[478] Online Article | Safehome | "Buying Guide for Home Security Cameras" | https://www.safehome.org/home-security-cameras/#features | accessed 19 June 2022

[479] Online Article | Digitaltrends | “Which smart security cams are serious about privacy? We’ve ranked them all” | July 16, 2021 | **https://www.digitaltrends.com/home/security-camera-scorecard-feature-comparison/** | accessed 19 June 2022
[480] Online Article | US News | “How to keep your home security cameras safe” | April 1, 2021 | **https://www.usnews.com/360-reviews/services/security-cameras/how-to-keep-your-security-cameras-safe** | accessed 19 June 2022
481 Website | SanctionScanner | “What is the Money Service Business?” | **https://sanctionscanner.com/knowledge-base/money-service-business-133** |accessed on 23 May 2022
[482] Website | Comply Advantage | “What Is A Money Services Business?” | **https://complyadvantage.com/knowledgebase/anti-money-laundering/money-services-business/** | accessed on 20 May 2022
[483] Website | PayPal | “Our privacy-first promise” | **https://www.paypal.com/myaccount/privacy/privacyhub** | accessed on 20 May 2022
[484] Online article | Finextra | “Twitter Tip Jar users cite PayPal privacy concerns hours after rollout” | 07 May 2021 | **https://www.finextra.com/newsarticle/38008/twitter-tip-jar-users-cite-paypal-privacy-concerns-hours-after-rollout**
[485] Online article | BleepingComputer – Ax Sharma | “Twitter Tip Jar may expose PayPal address, sparks privacy concerns” | 07 May 2021 | **https://www.bleepingcomputer.com/news/security/twitter-tip-jar-may-expose-paypal-address-sparks-privacy-concerns/**
[486] Website | Venmo | **https://venmo.com/about/us/** | accessed on 20 May 2022
[487] Online Article | EFF | “Venmo Takes Another Step Toward Privacy” | 21 July 2021 | **https://www.eff.org/deeplinks/2021/07/venmo-takes-another-step-toward-privacy**
[488] Website | PayPal | “PayPal Privacy Statement - The personal information we collect” | **https://www.paypal.com/webapps/mpp/ua/privacy-full#dataCollect** | accessed on 20 May 2022
[489] Website | Venmo | “Payment Activity and Privacy” | **https://help.venmo.com/hc/en-us/articles/210413717-Payment-Activity-Privacy** | accessed on 20 May 2022
[490] Online article | FCC | “Mobile Wallet Services Protection” | 25 February 2020 | **https://www.fcc.gov/consumers/guides/mobile-wallet-services-protection**
[491] Online article | Department of Justice | “Increased Use of Mobile Banking Apps Could Lead to Exploitation” | 10 June 2020 | **https://www.ic3.gov/Media/Y2020/PSA200610**
[492] Online Article | eFraud Prevention, LLC. | “Safeguard mobile wallet” | **https://efraudprevention.net/home/templates/?a=99** | accessed on 19 May 2022
[493] Online article | FCC| “Protect Your Smart Device” | 31 December 2019 | **https://www.fcc.gov/consumers/guides/protect-your-mobile-device**
[494] Online article | DigitalTrends | “How to remove location data from your iPhone photos” | 22 December 2021|**https://www.digitaltrends.com/mobile/how-to-remove-location-data-from-iphone-photos-in-ios-13/** | accessed on 27 June 2022
[495] Online article | XDA| “XDA Basics: How to view and remove EXIF data on Android and iOS, and stop Location Tagging”| 24 June 2021 | **https://www.xda-developers.com/how-to-view-remove-exif-data-android-ios/** | accessed on 27 June 2022
[496] Online Article | Apple Inc. | “Use Screen Time on your iPhone, iPad, or iPod touch” | **https://support.apple.com/en-us/HT208982** | accessed on 12 May 2022
497 Online article | Android Central | “How to remove location data from photos on Android” | 3 June 2020 | **https://www.androidcentral.com/how-remove-location-data-photos-android**
[498] Blog post | Backlight | "Google Photos and privacy: How to keep your photos safe" | 9 June 2020 | **https://backlightblog.com/google-photos-privacy**
[499] Website | Google Photos | **https://www.google.com/photos/about/** | accessed on 12 May 2022
[500] Online article | How-toGeek | “How to Hide People from Memories in Google Photos” | 21 May 2021 | **https://www.howtogeek.com/729788/how-to-hide-people-from-memories-in-google-photos/**
[501] Google | Website | "Watch & Manage Your Memories" | **https://support.google.com/photos/answer/9454489?hl=en&co=GENIE.Platform%3DAndroid#zippy=%2Ccontrol-which-memories-you-receive%2Chide-someone** | accessed on 20 May 2022