THE FREE COMPANION TO

UNDER CONSTANT SUPERVISION

RECLAIM YOUR PRIVACY

A GUIDE TO INCREASING YOUR DIGITAL PRIVACY AND SECURITY IN THE AGE OF SURVEILLANCE

THE FREE COMPANION TO **UNDER CONSTANT SUPERVISION**

RECLAIM YOUR PRIVACY

A GUIDE TO INCREASING YOUR DIGITAL PRIVACY AND SECURITY IN THE AGE OF SURVEILLANCE

BookRefine™
PUBLISHING

Reclaim Your Privacy
C.J. Thomson

Published by BookRefine Publishing, Australia

contact@bookrefine.com
Bookrefine.com
Design by ***CJCreative.design***

Every effort has been made to ensure that this publication contains accurate and current information at the time of its publication; however, the publisher and the author(s) shall not be liable for any loss, damage or liability as a result of the information contained herein. The views and opinions expressed in this book are those of the author(s) and do not necessarily reflect the position of the publisher. Any content provided or opinions are not intended to malign any religious or ethnic group, club, company, individual or government entity. All content is for educational and informational purposes only. The author(s) and publisher are not liable or responsible for any damages resulting from or related to your use of content featured within including -- but not limited to -- any suggestions or suspected encouragement that breaches local and international law.

All trademarks mentioned within the published works are acknowledged as belonging to their respected owners. This book may contain copyrighted material the use of which has not been specifically authorised by the copyright owner. We believe making such material available to advance understanding of user privacy, surveillance, censorship and technologies constitute 'fair use'

This work is creator endorsed under a strict set of guidelines aiming for a better copyright system and therefore all fairness between publisher and author(s) has been insured under the hope that these guides are respected by the consumer of such works.

We cannot guarantee that all links will work and cannot take responsibility for any changes to live pages.

(DE)GOOGLE

Trying to rely a little less on Google for services like maps and cloud storage was far from easy, especially given the amount of services one may not even realise belongs to Google or is partially owned by Google.

For me, the big effort would begin with removing myself from Gmail. And for me personally, it wasn't just a personal Gmail account – it was several email accounts attached to my business affairs through the Gsuite service – a service which gave me a one-stop shop for business email, storage and various productivity tools for myself and a small amount of people who may need access to help me operate my businesses. This was a service I had used since about 2007 when it was known as Google Apps for your Domain. It was initially free for small businesses like mine.

DeGoogling was never really on the cards for me, I enjoyed Google's products and was entirely unphased by any potential privacy concerns. It was Evernote I began to take issue with – and that was because the simple note-taking service had annoyed me with their device limits for free accounts. Nothing is truly free. I knew that, but paying $120 annually for a bunch of text files stored in the cloud that will STILL be subject to investigation should there ever be any suspicion on what I have or haven't done was not something I was willing to shell out money for.

I had nothing to conceal, but nothing to reveal.

When looking for alternatives to Evernote, I read into all the surrendered data that Evernote had supplied, including to authorities without correct permits or avenues sought for such data. I didn’t want to become another statistic. I didn’t want my personal notes to be sorted through by any entity just because they thought I might be a bit “different” with my independent publishing company. It was paranoid, but I felt I was given the right to be just a little bit concerned about my personal information. We all should be given that right.

I’d also heard from similar companies that Evernote made it increasingly difficult to migrate out of the service. That concerned me, especially with the expectation of big services to make it a right for anyone to choose to leave and take their personal data.

I realised that moving from Evernote was a bad idea… if I was to stick with Google. Several times over the past few years I have noticed that Google would ban me for periods of up to 24 hours due to my usage of enemy companies. For example, when adding Gmail accounts to both my desktop and laptop computers Thunderbird or Outlook mail clients, I would be smashed with security notices on all of my devices and then despite assuring my account was safe; I would still be locked out. This was bad for personal and business reasons as you can imagine.

I was also caught out using "untrusted" authenticator applications on my Android devices. Microsoft Authenticator and Bitwarden would both lock me out. When I raised this with Google, they suggested that it wouldn’t happen if I removed the Google accounts from those authenticators and opted for Google's versions instead.

As established earlier, Gmail monitors your content, email messages and combines that information with what they find in the rest of your linked Google Accounts. Even fitness tracker manufacturer and service Fitbit are now owned by Google with very little information provided on how that would potentially affect your personal data and if whatever was stored on Fitbit servers would be directly transferred to Googles'

It was quite scary to find that using a password I had on my account several years ago was still stored and triggered a security notice stating "you can't use a password that has previously been used on this account" or words to that effect.

I've previously complained about how Google's automated (and sometimes non-automated) systems have blocked my original music on YouTube from MY OWN profiles due to copyright complaints – some of which even stating my music was owned by companies like Warner Brothers and BMG – and I have also found that using Google Drive storage to send tracks to friends and music associates has also landed me in trouble.

Music I have written, published and maintained 100% ownership of. When raising this with Google, I have been given generic responses and been told that there was nothing I could do but they would investigate it. At one point I even received a copyright strike against my YouTube account – one of which took months to get rid of!

I acknowledged at the time that one cannot TRULY escape Google. I still have several Android devices and required connections to the company. There's only so far one can get with alternatives before having to resort to the official Google applications – especially with applications that are only available via the Google Play store.

Some things to get you started if you're navigating away from Gmail –and Google in general—:

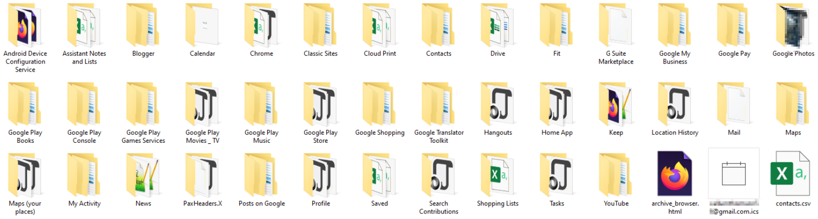
- You can grab an archive of all your data through **Google's Takeout service.**

- You can easily keep your Gmail address and have any emails from it forward to your new email by setting up email forwarding.

- **You can set up an autoresponder** to let people know that you have a new email address (and even let them know that you'll still get the email they sent as it'll forward on)

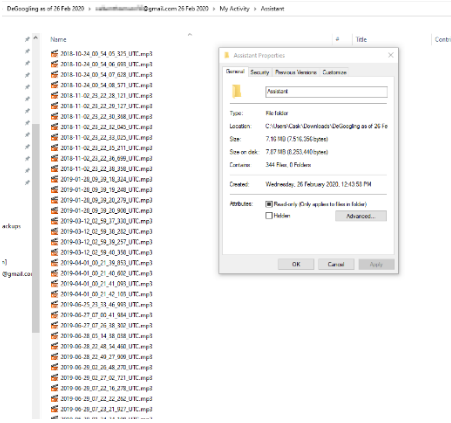
After moving away from Google, I decided I'd begin sifting through the data that was stored in my "Takeout" archive. This was a very interesting thing to do and showed me just how much of my life was stored in Google's data centres.

After deciding to dump Google (or as much as I could, at least) I figured I'd go through the export of my main personal account that I have had for many years.



It's no surprise that Google had tons of information stored on their servers about my life and day-to-day activities. After all, I uploaded the entries and enabled them to do so by not taking better care of what activity I had set in the accounts but it's still quite overwhelming to go through roughly 15 years of data and see what types of information have been kept all this time -- most of which has either been removed due to expiry or data loss or otherwise.

Every voice input into Google Assistant -- both intentional and accidental -- since 2017 set out beautifully across multiple folders. Some of these recordings begin BEFORE I am heard saying "Hey Google!"



DeGoogling as of 26 Feb 2020 > [redacted]@gmail.com 26 Feb 2020 > My Activity > Assistant

ackups

n]

@gmail.co

```
Name
2018-10-24_00_54_05_325_UTC.mp3
2018-10-24_00_54_06_693_UTC.mp3
2018-10-24_00_54_07_628_UTC.mp3
2018-10-24_00_54_08_571_UTC.mp3
2018-11-02_23_22_28_121_UTC.mp3
2018-11-02_23_22_29_127_UTC.mp3
2018-11-02_23_22_30_368_UTC.mp3
2018-11-02_23_22_32_045_UTC.mp3
2018-11-02_23_22_33_025_UTC.mp3
2018-11-02_23_22_35_211_UTC.mp3
2018-11-02_23_22_36_699_UTC.mp3
2018-11-02_23_22_38_358_UTC.mp3
2019-01-28_09_39_18_324_UTC.mp3
2019-01-28_09_39_19_248_UTC.mp3
2019-01-28_09_39_20_279_UTC.mp3
2019-01-28_09_39_20_900_UTC.mp3
2019-03-12_02_59_37_330_UTC.mp3
2019-03-12_02_59_38_282_UTC.mp3
2019-03-12_02_59_39_257_UTC.mp3
2019-03-12_02_59_40_358_UTC.mp3
2019-04-01_00_21_39_853_UTC.mp3
2019-04-01_00_21_40_602_UTC.mp3
2019-04-01_00_21_41_093_UTC.mp3
2019-04-01_00_21_42_103_UTC.mp3
2019-06-25_23_33_46_993_UTC.mp3
2019-06-27_07_00_41_984_UTC.mp3
2019-06-27_07_26_38_302_UTC.mp3
2019-06-28_05_14_38_038_UTC.mp3
2019-06-28_22_48_54_460_UTC.mp3
2019-06-28_22_49_27_909_UTC.mp3
2019-06-29_02_26_48_270_UTC.mp3
2019-06-29_02_27_02_721_UTC.mp3
2019-06-29_07_22_16_278_UTC.mp3
2019-06-29_07_22_22_262_UTC.mp3
2019-06-29_07_23_21_927_UTC.mp3
```

Assistant Properties

General | Security | Previous Versions | Customize

Assistant

Type: File folder

Location: C:\Users\Cask\Downloads\DeGoogling as of 26 Fe

Size: 7.16 MB (7,516,356 bytes)

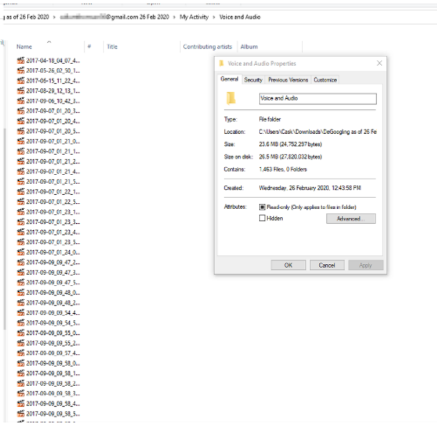
Size on disk: 7.87 MB (8,253,440 bytes)

Contains: 344 Files, 0 Folders

Created: Wednesday, 26 February 2020, 12:43:58 PM

Attributes: ☒ Read-only (Only applies to files in folder)

☐ Hidden



as of 26 Feb 2020 > [redacted]@gmail.com 26 Feb 2020 > My Activity > Voice and Audio

```
Name
2017-04-18_04_07_4...
2017-05-26_02_50_1...
2017-06-15_11_22_4...
2017-08-29_12_13_1...
2017-09-06_10_42_3...
2017-09-07_01_20_3...
2017-09-07_01_20_4...
2017-09-07_01_20_5...
2017-09-07_01_21_0...
2017-09-07_01_21_1...
2017-09-07_01_21_2...
2017-09-07_01_21_4...
2017-09-07_01_21_5...
2017-09-07_01_22_1...
2017-09-07_01_22_5...
2017-09-07_01_23_1...
2017-09-07_01_23_3...
2017-09-07_01_23_4...
2017-09-07_01_23_5...
2017-09-07_01_24_0...
2017-09-09_09_47_2...
2017-09-09_09_47_3...
2017-09-09_09_47_5...
2017-09-09_09_48_0...
2017-09-09_09_48_2...
2017-09-09_09_54_4...
2017-09-09_09_54_5...
2017-09-09_09_55_0...
2017-09-09_09_55_2...
2017-09-09_09_57_4...
2017-09-09_09_58_0...
2017-09-09_09_58_1...
2017-09-09_09_58_2...
2017-09-09_09_58_3...
2017-09-09_09_58_4...
2017-09-09_09_58_5...
```

Voice and Audio Properties

General | Security | Previous Versions | Customize

Voice and Audio

Type: File folder

Location: C:\Users\Cask\Downloads\DeGoogling as of 26 Fe

Size: 23.6 MB (24,752,297 bytes)

Size on disk: 26.5 MB (27,820,032 bytes)

Contains: 1,463 Files, 0 Folders

Created: Wednesday, 26 February 2020, 12:43:58 PM

Attributes: ☒ Read-only (Only applies to files in folder)

☐ Hidden

Some of the data is simply anonymised rather than deleted. As per Google's privacy policy under "How Google retains data…":

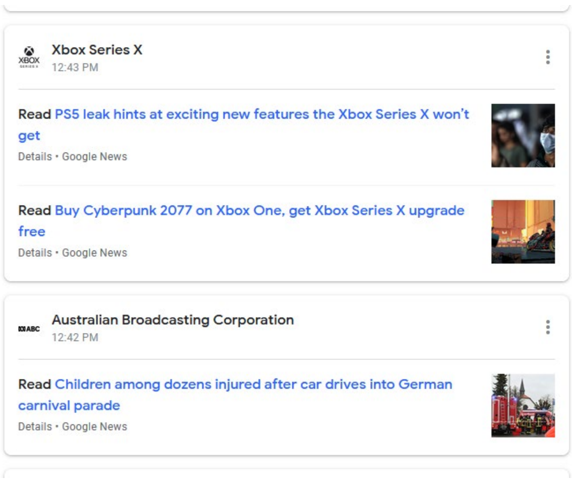
> *In some cases, rather than provide a way to delete data, we store it for a predetermined period of time. For each type of data, we set retention time frames based on the reason for its collection. For example, to ensure that our services display properly on many different types of devices, we may retain browser width and height for up to nine months. We also take steps to make certain data anonymous within set time periods. For example, we make advertising data in server logs anonymous by removing part of the IP address after nine months, and cookie information after 18 months.*

And:

> *For example, after you delete a specific Google search from My Activity, we might keep information about how often you search for things, but not what you searched for.*

To be fair, you can disable the activity, or have it set that the activity is deleted after 3 months, but the defaults are something people often overlook. Google doesn't make it any easier with its consistent warnings that by deleting or disabling the activity history you'll essentially break every service you use. According to Google's help pages on the subject, your data is deleted from your view and may be retained for a duration they see fit.

Google has a cleverly worded video that makes all this seem a little less creepy - though liking/disliking the video or commenting is disabled.



Xbox Series X
12:43 PM

Read PS5 leak hints at exciting new features the Xbox Series X won't get
Details • Google News

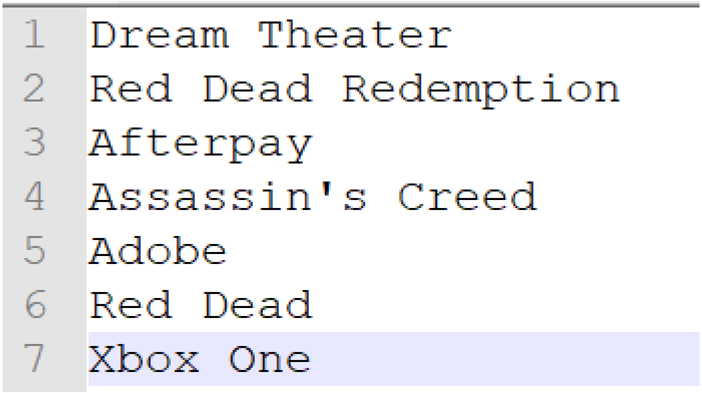
Read Buy Cyberpunk 2077 on Xbox One, get Xbox Series X upgrade free
Details • Google News

Australian Broadcasting Corporation
12:42 PM

Read Children among dozens injured after car drives into German carnival parade
Details • Google News

Every article I have ever read via Google News and, more concerningly, every article I didn’t want to read. If I didn’t know the user of the account, I'd be able to perfectly handcraft a description of his or her political associations and beliefs, taste in music (even though I didn't use Google Play music), preferred applications and even applications I have searched or viewed in the store. I had also searched for medication prices using Google Search and this would assist in painting the picture of the medication I may be on or have been on previously and the conditions I may have or had. Suddenly the idea of the masses referring to Dr Google gives another worrying prospect.

Further inspection into my infrequent use of the Google News aggregator shows they at least managed to discover what games, software and music I liked to know about:

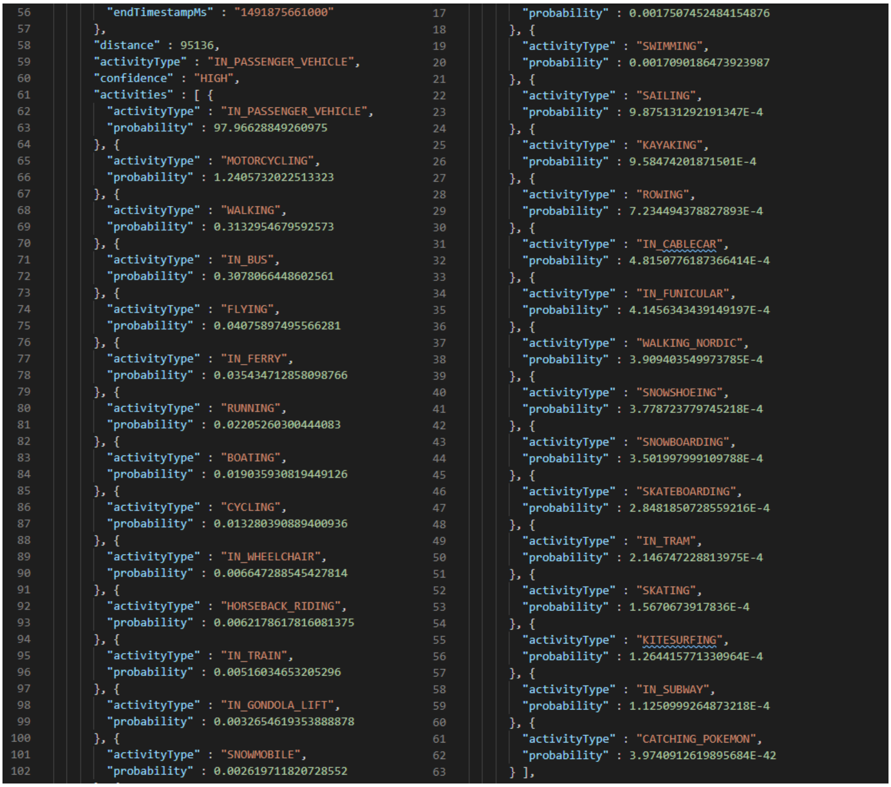


```
Dream Theater
Red Dead Redemption
Afterpay
Assassin's Creed
Adobe
Red Dead
Xbox One
```

I never really used most of Google's features and yet the profile built around my usage of the few I did has created some interesting connections within the Google Takeout archive. Kudos to Google for allowing me to see it all, even though it's my basic right as an account holder - but it's what they don't reveal (if so) that has me wondering now. Google's "My Activity" dashboard likes to remind the user that "Only you can see this data"

SERVICES YOU MAY NOT HAVE USED

I have never used Google Fit, yet there is plenty of data stored suggesting I used an application that must have linked to it from May to September of 2019. I use a Fitbit watch (which will be dismissed in favour of something a bit more private, which seems like a bit of an oxymoron) – as far as I can tell, the Google Fit data isn’t consistent with the information that Fitbit has collected during the same period, leading me unable to connect it to Google’s buyout of Fitbit, Inc which was announced several months after said data collection has stopped. Mysteriously though, I have never used any fitness tracking application or device other than the official Fitbit application and the Fitbit Versa, respectively. The .tcx files (which are essentially XML files) contain suggestions that Garmin are related to the data. Some basic research suggests Pokémon Go and its “Adventure Sync” could be the culprit but I ceased playing that several years ago. Your guess is good as mine, but it demonstrates the reach of Google, their affiliates and any applications you use that could be sharing data to Google.



```
      "endTimestampMs" : "1491875661000"
    },
    "distance" : 95136,
    "activityType" : "IN_PASSENGER_VEHICLE",
    "confidence" : "HIGH",
    "activities" : [ {
      "activityType" : "IN_PASSENGER_VEHICLE",
      "probability" : 97.96628849260975
    }, {
      "activityType" : "MOTORCYCLING",
      "probability" : 1.2405732022513323
    }, {
      "activityType" : "WALKING",
      "probability" : 0.3132954679592573
    }, {
      "activityType" : "IN_BUS",
      "probability" : 0.3078066448602561
    }, {
      "activityType" : "FLYING",
      "probability" : 0.04075897495566281
    }, {
      "activityType" : "IN_FERRY",
      "probability" : 0.035434712858098766
    }, {
      "activityType" : "RUNNING",
      "probability" : 0.02205260300444083
    }, {
      "activityType" : "BOATING",
      "probability" : 0.019035930819449126
    }, {
      "activityType" : "CYCLING",
      "probability" : 0.013280390889400936
    }, {
      "activityType" : "IN_WHEELCHAIR",
      "probability" : 0.006647288545427814
    }, {
      "activityType" : "HORSEBACK_RIDING",
      "probability" : 0.0062178617816081375
    }, {
      "activityType" : "IN_TRAIN",
      "probability" : 0.00516034653205296
    }, {
      "activityType" : "IN_GONDOLA_LIFT",
      "probability" : 0.0032654619353888878
    }, {
      "activityType" : "SNOWMOBILE",
      "probability" : 0.002619711820728552
```

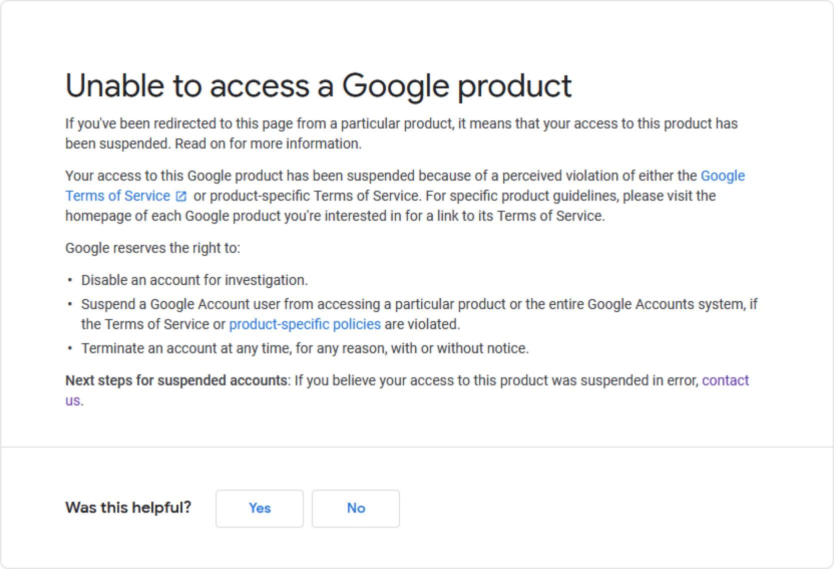
```
      "probability" : 0.0017507452484154876
    }, {
      "activityType" : "SWIMMING",
      "probability" : 0.0017090186473923987
    }, {
      "activityType" : "SAILING",
      "probability" : 9.875131292191347E-4
    }, {
      "activityType" : "KAYAKING",
      "probability" : 9.58474201871501E-4
    }, {
      "activityType" : "ROWING",
      "probability" : 7.234494378827893E-4
    }, {
      "activityType" : "IN_CABLECAR",
      "probability" : 4.8150776187366414E-4
    }, {
      "activityType" : "IN_FUNICULAR",
      "probability" : 4.1456343439149197E-4
    }, {
      "activityType" : "WALKING_NORDIC",
      "probability" : 3.909403549973785E-4
    }, {
      "activityType" : "SNOWSHOEING",
      "probability" : 3.778723779745218E-4
    }, {
      "activityType" : "SNOWBOARDING",
      "probability" : 3.501997999109788E-4
    }, {
      "activityType" : "SKATEBOARDING",
      "probability" : 2.8481850728559216E-4
    }, {
      "activityType" : "IN_TRAM",
      "probability" : 2.146747228813975E-4
    }, {
      "activityType" : "SKATING",
      "probability" : 1.5670673917836E-4
    }, {
      "activityType" : "KITESURFING",
      "probability" : 1.264415771330964E-4
    }, {
      "activityType" : "IN_SUBWAY",
      "probability" : 1.1250999264873218E-4
    }, {
      "activityType" : "CATCHING_POKEMON",
      "probability" : 3.9740912619895684E-42
    } ],
```

GOOGLE PLAY CONSOLE:

My Google Play developer console folder has several applications and versions that I removed when I ceased using my developer account. Whilst they haven't stored (or returned) the application files and source code, I see a history of application updates and application build attempts. Change logs and other information submitted is retained from 2015 – the date that I removed all the applications from my account and from download and relocated them to my Google business account.

Visiting the Developer Console reveals that there is absolutely nothing available to touch and that I am only able to upload a new application. There is nothing to delete.

I contacted Google and was informed I would have to contact their privacy team to request removal of the data that had appeared in my Takeout. Since doing this, it seems I am entirely unable to even visit my developer console. I am now redirected to a page that suggests I was banned from the service:



Unable to access a Google product

If you've been redirected to this page from a particular product, it means that your access to this product has been suspended. Read on for more information.

Your access to this Google product has been suspended because of a perceived violation of either the Google Terms of Service or product-specific Terms of Service. For specific product guidelines, please visit the homepage of each Google product you're interested in for a link to its Terms of Service.

Google reserves the right to:

- Disable an account for investigation.
- Suspend a Google Account user from accessing a particular product or the entire Google Accounts system, if the Terms of Service or product-specific policies are violated.
- Terminate an account at any time, for any reason, with or without notice.

Next steps for suspended accounts: If you believe your access to this product was suspended in error, contact us.

It doesn’t stop there. I did another Google Takeout – and the data was still there. I contacted Google’s privacy team again and received a canned response a few hours later simply stating the data cannot be removed and that it was secure and anonymised as per their policies. From that, I assume that deleting my account completely will not remove the information stored. I suspect that intentionally getting myself banned from Google by breaking their rules will not help either. Luckily, I have nothing to hide and that all the information is useless to me and everyone outside of my life – but that doesn't mean it is okay! Although things such as my email address and phone number are present within the files. Some of the data Google have provided has not actually been unencrypted upon extraction. For example, my various preferences and settings .json files are filled with unusable information.

I contacted Google and authorised them to provide me with the data that has been unencrypted. They can't help with that apparently.

Furthermore, I noticed that some contact information was available in the "`team_members.json`" – this included a couple of people I had been developing applications with who had access to the account. It seems their data will remain too.

DEVICES:

Despite having removed the retired devices from the multitude of Google services over the years, it appears that some – but not all – devices are contained within the archive. From an old smart TV I logged into last year and subsequently removed from my account after realising I didn't need the features Android would offer me, to a Samsung SII I had back in 2011; it's all still here complete with IMEI numbers, Android ID's, device serial numbers and even the IP address from the date of its last connection whilst associated with my account.

Information including first data connection times, SIM operators and applications installed are all featured within an extensive HTML document. If you visit Google's "Your

Devices” dashboard, you’ll see every device you currently have connected to your account. From there, you can locate a device (which is a great feature) and remove any old devices you are signed in to. You can also see the devices you have signed in or registered to your account on the Google Play settings page (though you cannot remove them)
But what about the devices you have signed out from or formatted for resale or recycling? Well on that same page you will find any device you have signed out of…in the last 28 days.

There is absolutely no mention of any device that you have linked that Google still holds the information to such as those I found in my data export.
I also found that I had a device that was replaced under warranty a few days after I activated it. The device isn’t shown anywhere in my account, but the long page of information Google has on it remains.

As of writing, it appears that there is no method to remove those old unused devices from your account. If you’re concerned about your security, change your password. If you’re concerned about the fact that Google has records of these devices on their servers, complete with information such as the applications you installed, networks used and so on then you can wait for the dormant device to be removed from your account automatically…but, as was in my case, this doesn’t seem to apply to all of them. Once again, it seems like Google will let you hide something from view, but ultimately continue storing any data collected. Google’s own support page seemingly glosses over that little fact.

Navigating to the “My Activity > Android” folder gave me an insight into how much application usage is stored. From opening the file manager and deleting some junk downloads, to opening an image application and viewing some viral videos; it's all here and clear.

ADVERTISEMENTS:

This was always going to be an unsurprising discovery but as somebody who doesn't exactly click on every advertisement they see, it was amazing to see the thousands of entries over the past decade that told me what I clicked, the URL it led to and the date and time I clicked on it. Even the advertisements I wouldn't have visited intentionally – such as those that were thrown at me by an Android app – are included.

LOCATION HISTORY:

My location history contained at least 300 different locations and routes that I had used through the Google Maps application on my phone and any searches I had done on my desktop.

There is a pile of files in the "Semantic Location History" that give me insight into what was collected. Opening these .json files up in Visual Studio (code editor - you can use Notepad++ or the free Visual Studio Code if you want to dig through your own .json extractions) shows me the calculations (or "probability") of my movements:

Also, take note of the "CATCHING_POKEMON" estimation!

The specifics of vehicles I was potentially driving or passenger in are even noted. For example: IN_ROAD_VEHICLE and IN_FOUR_WHEELER_VEHICLE.

One of these location files was a whopping 281MB. If you're doing this yourself and have huge files of mass text too then you'll want to be using 64-bit software with a decent enough computer. Even then, expect some crashing!

That's a lot of text. With word-wrapping enabled in Visual Studio, that's 12,517,808 lines of text. To put that into perspective by using words, that's a total of twelve million, five hundred and seventeen thousand, eight hundred and eight lines. All up about 17 million words and I'd estimate about 12-14 million of that is personal location data if I take all the random accuracy and prediction lines into consideration.

Despite thinking that I had disabled location tracking, it turns out that in order to completely stop Google from logging coordinates, I had to dive a little deeper and disable ***web and app activity.***

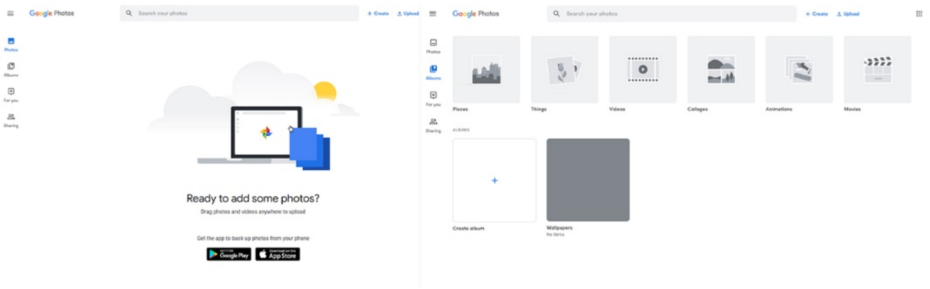
Again, in total acknowledgement, I could have stopped Google from keeping all my location history by taking a proper look at what data collection I had set – but it seems like many settings are intentionally misleading even to those who consider themselves advanced computer users.

PHOTOS:

Despite never using Google's services to upload personal photos – I was, for a time, a big contributor of professional photography to Panoramio even prior to Google's purchase and later discontinuation of the product – but it's the things like profile pictures, YouTube thumbnail uploads and similar that make up a folder filled with metadata even if you deleted the images. Thankfully, photos dating as far back as 2004 that have long-since been deleted are not present, but their metadata is. Within each of the 750 directories is the information for images I have emailed or uploaded to my account. Even figures for images within email signatures are included.

I don't tend to upload photographs with geolocation data embedded, but for those that were uploaded and later deleted, the .json files reveal the coordinates that were attached. As of writing, Google Photos gives users unlimited storage for high quality photos and videos at no [financial] cost. I'll let you conclude why.

With all these files and their information available to me in my extracted archive, I will show you what is contained in my online Google Photos account:



Ready to add some photos?

Drag photos and videos anywhere to upload

Get the app to back up photos from your phone

That's right. Absolutely nothing. Or well so I thought and so it would seem to most…

Investigation into the "My Activity" folder showed me the likely-overseen fact that closing a suggestion, swiping away an article on your connected device or accessing a website, application or viewing content anywhere via one of Google's many services creates a log that tells Google what you are and aren't interested in seeing. From a usefulness point-of-view, I entirely understand that – but when that information can be used to suggest things like, for example, you don't care about what Meghan Markle has to say about the Royal Family – it paints a picture that is incredibly valuable to Google and their associates. It surprises me that there wasn't a log of every event in my calendar that I had cancelled or postponed. Combine that with an entry in my location history and you could almost frame me for something in which I was not involved. So that leads me to my next paragraph:

Google's Privacy Principles seem great. According to their Safety Centre, they vow to Respect their users and privacy, never sell personal information (the claim is that their free services are funded by relevant advertising) and empower people to remove their data should they wish. If "leading by example" is their wish, then we are in trouble. I am still in my early stages and I doubt I'll ever be truly rid of Google – short of becoming a hermit who hides in the wilderness – but I have taken the early steps and it's quite an interesting and redeeming experience. Dare I say it's my first digital awakening in a journey of self-exploration?

I encourage you to take the first leap by removing yourself from one of your most-used Google services. I'm not suggesting you completely rip Google out of your life right now but consider the reality that giving Google less of your information will give you more control over your private life.

I think the first baby step is to download an archive of your information and see for yourself what the company is storing:

If you want to go through the data that Google has so-considerately maintained in a massive database, then login and head to ***https://takeout.google.com/***
I recommend setting your export to split files, as I've found that the downloads like to timeout and there's a limit to how many retries you get before having to request another export.

A lot of the files may be empty or contain no actual information. For example, if you have never used Google Chrome, you're still likely to be given a bunch of files that don't have anything to say – or you'll get a lovely set of document that feature multiple lines saying "Your data is encrypted and cannot be exported"

This is pure speculation, but should that information be accessed by a hacker, law enforcement agency or other interested party; will they be able to label you a racist for not caring about what a politician had to say about neo-Nazism or discrimination of ones' race? Will you be attributed as heartless – whether by person or machine – for swiping away that advertisement about the dying children in Africa needing your help? And will you find yourself facing the consequences of watching legal pornography or for spending a few minutes on a page where the author has expressed their opinion on something considered 'dangerous' to society?
You don't need to abandon the helpful services on the internet or install an incredibly secure version of Linux in an underground bunker if you wish to casually use your personal devices and technology without giving away unnecessary information that doesn't benefit you.

Some of the information in this part of the book may seem a little obvious to you depending on your technological expertise. Each application and website listed has been personally verified to ensure that it is secure and offered by the developers with zero or minimal commercial incentive. Many of these applications are open-source (released free with source code released under a license in which the copyright holder grants users the rights to study, change, and distribute the software or collaborate openly) whilst free and paid applications are labelled as such.

A list of links is included for those looking to download their data from various providers. This is by no-means a comprehensive and complete list.

Furthermore, a list of useful websites is also included that can help you examine, remove or control your online presence. Any site that requires registration or verification is labelled appropriately.

You'll see GitHub mentioned several times. For those of you who are unaware of GitHub, it's a developer website for open-source collaboration. For the purpose of the book, it is used as a trustworthy location to find many applications, links and lists that are freely accessible to all.

It should go without saying that the internet is dynamic, and some links may no longer work or provide the purpose described below. As a result, many of the suggestions include only services and applications that have been around for a long duration of time.

THINGS TO CONSIDER WHEN SIGNING UP ONLINE:

Duration of service: You don't want to discount any company for being new, but at the same time you want to know they'll stick around and that if they close, you will know about it and have access to your data and that it will be destroyed when they liquidate. Most Terms of Service or Terms and Conditions pages will call this an End of Life, or EOL, policy.

Mergers and Buyouts: Always check the policies for what would happen if the company was bought-out or merged with another entity. You want to be assured that you're agreeing to a contract that states the business taking over will be forced to abide by the terms and policies you agreed to when signing up.

Cloud content / User data: Is it okay to upload pirated content and pornography, if you're not going to share it publicly – I'll admit this is a weird one. I sought it not because I was going to be storing anything of the sort, but if a company has reason to terminate your service for such things, then chances are they're using manual and/or automated systems to scan your content.

Companies like Google are well-known for sifting through your uploads to find copyrighted works. Dropbox can automatically find copyrighted materials within your private account and prevent you from sharing them. Surely you don't want companies going through any of your cloud-hosted content no matter what the method? Most of the time infringing content is to be removed after the copyright holder requests it.

This does not mean that there is a mandate to search through user information to prevent it. In short: companies don’t have to oblige, but they do have to cooperate. Is going through your uploads part of that cooperation? That’s for you to consider.

Read the terms and conditions and privacy policies of every service. A lot of the time speedreading or scanning through the pages with page search just to see what the policies state about specific circumstances such as content they deem objectionable can be incredibly useful.

It may sound a little contradictory, but when aiming to maintain your privacy when using services, operating systems and hardware devices consider the possibility that you are not always monitored for unethical purposes.
Smart devices such as home automation units and digital assistants may be using your data to improve their services, but not always. Sometimes when a company claims they use the data to improve how the software responds to you in particular they aren't trying to justify any sort of spying. This is why reading through privacy policies is so important. There are many transparent, open companies out there that only use anonymised data to fix bugs and improve the software.

Consider the intentions of the company or software developer and the transparency of why they use your data. Whilst there are always reasons to question the honesty of the claims written in a Privacy Policy, the potential fines for misrepresenting a legal document often exceed the value of a small company and its product. Government agencies linked to the worst offenders of surveillance may be behind the laws set out to protect users, but several organisations exist to ensure that companies and developers play by the rules no matter how powerful they are.

To give a personal perspective: I have my finger in many pies. I'm a musician who uses the data of website visitors and streaming service listeners to understand how I was discovered, where the listener came from and other artists the user has listened to. This data is valuable only for the purpose of curiosity and the hope that I can reach a wider audience by making my music available to those who are more likely to appreciate it. As a small application developer, I've used statistics and logs to fix bugs, focus on the Operating System of the computer or device used and attempt to understand the most-used features of the software so that I can prioritise the improvements for where they will be appreciated most.

As the founder of the very company that has published this book, I have collected information valuable only for the purposes of promoting the books, understanding the periods of the year that sales increase and how the customer was directed to the book or website containing inf or reviews on it. This information is collected and is not sold to any third party. I'd assume the data is worthless to anyone other than the business.

DOWNLOAD YOUR DATA

DIGITAL DATA ARCHAEOLOGY

Downloaded files may contain confidential content, such as search and location history, and other personal data, sometimes exposed passwords and unencrypted information. It is best not to download your archive to a public computer or anywhere it can be accessed by unauthorised persons. Many of these archives are compressed as .zip files which can be opened natively by many Operating Systems such as Windows. Data files included such as .json can be opened with inbuilt notepad applications.

If you are concerned about the data stored on your computer or anywhere else, you can extract it and then archive it again – with a password – with the compressed archive software suggested.

These free, trustworthy tools are suggested for accessing and viewing the data contained within the exports:

Opening compressed archives:

7zip	https://www.7-zip.org/
PeaZip	https://www.peazip.org/

Opening most text-based files (such as .json, .xml...):

Notepad++	https://notepad-plus-plus.org/
VSCode*	https://code.visualstudio.com/

* Owned by Microsoft but free and available on MacOS

EXPORTING YOUR DATA

This is a small guide to exporting your data from major companies:

GOOGLE:

1. Go to https://takeout.google.com/
2. Log in
3. Select the data you'd like to export
4. Choose "***next step***"
5. Choose the method and frequency in which you'd like the data exported.

FACEBOOK:

1. Go to https://www.facebook.com/your_information/
2. Log in and verify account
3. Select "**Download your information**"

MICROSOFT:

1. Go to https://account.microsoft.com/privacy/activity-history
2. Log in and verify account
3. Select "**Download your data**"
    i. Note: you can also clear any history and information by going to the ***Privacy Dashboard*** https://account.microsoft.com/privacy

TWITTER:

1. Go to your Account settings by clicking on the more icon in the navigation bar and select **Settings and privacy** from the menu.
2. Under the Account section, click **Your Twitter data**.

3. Enter your password under **Download your Twitter data**, then click Confirm.

APPLE:

1. Sign in to your Apple ID account page at appleid.apple.com on a Mac, iPhone, iPad or PC.
2. Go to **Data & Privacy** and select **Manage Your Data and Privacy.**
3. On the following page, go to **Get a copy of your data** and select **Get started**
4. Select the specific sets of data you would like to download, such as calendar, iCloud contacts and App Store purchase history. You can also download everything by clicking “select all.”
5. Apple will then verify your identity and start organizing your data.
    a. Note: this can take several days, even weeks.

INSTAGRAM:

From Instagram on the Web:

1. Go to your profile and click the settings icon ⚙.
2. Click **Privacy and Security**.
3. Scroll down to **Data Download** and click **Request Download**.
4. Enter the email address where you'd like to receive a link to your data and enter your Instagram account password.
5. You'll soon receive an email titled **Your Instagram Data** with a link to your data. Click **Download Data** and follow the instructions to finish downloading your information.

From iOS or Android:

1. Go to your profile and tap **the menu icon**.
2. Tap **Settings**.
3. Tap **Security** and navigate to **Download Data**.
4. Enter the email address where you'd like to receive a link to your data and tap **Request Download**.
5. Enter your Instagram account password.
6. You'll soon receive an email titled **Your Instagram Data** with a link to your data. Click **Download Data** and follow the instructions to finish downloading your information.

SNAPCHAT:

1. Log into your account on accounts.snapchat.com
2. Click '**My Data**'
3. Click '**Submit Request**' at the bottom of the page
4. If you have verified an email address with Snapchat, we'll send you an email with a link once your data is ready to download
5. Follow the link in your email to download your data
6. Click the link to download your data

UBER:

1. Go to: https://myprivacy.uber.com/privacy/exploreyourdata/download
2. Log in and verify account
3. Wait for the data to be sent

Alternatives to Google and its services‹

In no particular order, here are a list of trusted services that can replace many of the Google features without too much disruption.

SEARCH ENGINES:

Note: many of these search engines are in-fact sourcing their results from major engines such as Google and Bing, but without the tracking and privacy violations.

- **DuckDuckGo** (https://duckduckgo.com) is a private search engine based in the United States. It is considered one of the fastest and most-secure engines but being based in the US may bring along with it some issues as will be investigated within the book.
- **Searx** (https://searx.me) labels itself as a privacy-respecting metasearch engine. The code is open-source meaning it is available to all developers.
- **Swisscows** (https://swisscows.com) is a Swiss-based search engine that is hosted in a James Bond-like data centre within the Swiss Alps known as "Swiss Fort Knox" considered to be the 'safest data centre in Europe'
- **Qwant** (https:// qwant.com) is another privacy-orientated engine with promises of no tracking. They are based in France.
- **Ecosia** (https:// ecosia.org) puts a bit of a spin on the traditional search engine by boasting servers that are powered by 100% renewable energy. The company also anonymises all searches within a week and uses profits to plant trees. Reports are made public proving such philanthropy. Based in Germany.

- **Givero** (https://givero.com) like Ecosia, Givero raises money for causes, this time selected by the user or dispersed evenly amongst climate charities, animal protection and even non-profit organisations such as Mozilla Foundation, the company behind Mozilla Firefox. Givero is based in Denmark.
- **Mojeek** (https://mojeek.com) is based in the United Kingdom and is a search engine that has its own crawler and index, meaning the results are entirely dedicated and separated from providers like Google and Microsoft's Bing. Again, a word of warning that the company is based within a country with poor privacy practices.

EMAIL PROVIDERS:

- **Tutanota** (https:// tutanota.com) is a private and secure service based in Germany. Accounts with up to 1GB of storage are free.
- **Mailfence** (https://mailfence.com) is a Belgian service. Accounts with up to 500MB of storage are free.
- **ProtonMail** (https://protonmail.com/) is a Swiss email provider that offers 500MB of free storage. Government entities and United States Venture Capital investors have been shown to fund ProtonMail in the past and so that should be researched before committing.
- **Runbox** (https://runbox.com) is based in Norway. They offer a 30-day trial.

CLOUD STORAGE:

If you're concerned about maintaining as much privacy and security as possible, then self-hosting a file sharing and cloud platform is the best way to go with open-source services such as Nextcloud (https://nextcloud.com) being amongst the most feature-filled and trusted.

More ideas continue in ***VIRTUALLY DISAPPEAR FROM THE CLOUD***

If this isn't a major concern for you then the following alternatives come highly recommended:

- **Tresorit** (https://tresorit.com/) are based in Switzerland and offer an easy-to-use platform for users and businesses
- **Sync** (https://sync.com/) also provide securely encrypted file transfer and cloud storage.

Dropbox, OneDrive, Box.com and various similar services are all good options if you’re using the providers for general storage. They are fairly secure, run by somewhat-trustworthy companies but may not exactly be the most private of options. At the end of the book is a guide for what to look at within the Terms of Service and Privacy Policy documentation for services such as these.

WEB BROWSERS:

All suggestions here are for free software.

How private is your web browser and any extensions you have attached to it? Simply visiting one of the following sites will give you a report on how private your browser is and what data can be (potentially) collected:

Electronic Frontier Foundation (EFF) Browser Test:
https://panopticlick.eff.org/

TentaVPN Browser Test:
https://tenta.com/test/

GeoTek Web Privacy Check:
https://ipinfo.info/html/privacy-check.php

The following extensions are incredibly light and ensure that various tracking, advertisements and data collection is blocked.

uBlock Origin

Blocks ads, elements you don't want to see and tracking servers. Uses community-built filter lists so that you can pick what you want to block. For example, if you want to block trackers but you are okay with certain websites displaying advertisements to monetise their content; you don't have to disable the addon throughout the whole website. You can specify that you want to keep the ads but block the trackers.

https://github.com/gorhill/uBlock

Disconnect

Amusingly, a privacy protection company that was built by former Google engineers. They offer commercial services such as VPNs, but they have a free (or pay what you want) extension for Chrome, Firefox and Opera. The extension can be used with other blockers with little issue.

https://disconnect.me/disconnect

DuckDuckGo Privacy Essentials

Developed by the same folk behind the search engine. It's a great light application. It grades websites and lists the trackers or potential concerns present on the website you are viewing.

https://github.com/duckduckgo/duckduckgo-privacy-extension

Privacy Badger

Another automatic tracking blocker. Privacy Badger was developed by the Electronic Frontier Foundation

https://www.eff.org/privacybadger

Decentraleyes

Content Delivery Networks (CDNs) allow website owners to process scripts on websites closer to the user in order to help with load times and decrease heavy bandwidth on their servers. This can cause privacy concerns, especially if a large third-party company is providing the CDN . Decentraleyes investigates HTML data and replaces external requests to CDNs if it discovers a known JavaScript library. This way the CDN never receives the request. Don't understand what any of this means? Then, still, get the extension!

https://decentraleyes.org/

HTTPS Everywhere
Another great extension by the EFF. HTTPS everywhere is a lightweight add-on that ensures you're always using the encrypted site when available.

https://www.eff.org/https-everywhere

Mozilla Firefox with some additional extensions will make for a faster, safer browser. If you're concerned about certain websites tracking you, **Brave browser** is a fantastic choice and in 2020 was labelled "the most secure" by multiple technology outlets. The company behind it, Brave Software, was founded by creator of Javascript and former CEO of Mozilla Corporation Brendan Eich.

USEFUL WEBSITE TOOLS TO KEEP YOU SAFE AND ALERT:

Terms of Service; Didn’t Read
TOS;DR Gauges websites and how fair their Terms of Service and Privacy Policies are and lists issues that are of concern. Everything is graded using a classification system and colour-coded badges to visualise whether or not a services’ TOS or PP is clear and respectable. Available for download on GitHub

https://tosdr.org/
https://github.com/tosdr/

Just Delete Me
Features a directory of links that lead you to the area where you can delete your account. Just Delete Me also gauges how difficult it is to remove your account and data from the service – handy if you’re considering whether to join in the first place. The website is also available for download on GitHub.

https://justdeleteme.xyz/
https://github.com/jdm-contrib/jdm

Have I been pwned?
Simply insert an email address and it will search through known privacy breaches for the address. You’ll need to register to find out a bit more about any breaches.

https://haveibeenpwned.com/

Firefox Monitor
Whilst the data is provided by Have I Been Pwned, Firefox Monitor goes a few steps further. It requires a Firefox account and email confirmations for any emails you want to search but you'll get an in-depth look into any breaches and security concerns for the email addresses you've elected to monitor.
https://monitor.firefox.com/

PRISM-Break features a list of secure alternatives to popular software and services:
https://prism-break.org/en/

AlternativeTo is a user-collaborative directory of alternative software
https://alternativeto.net/

WINDOWS 10

When Windows 10 launched it had a whole host of controversial telemetry and data-collecting methods preinstalled that caused concern for many users.
Since then, Microsoft has attempted to redeem the trust of those accusing them of creating software designed to collect personal information through the potential false-pretence of "improving services"

Despite their attempts to make their data collection more transparent and giving users the ability to control what data is shared, there are many features lurking within Windows 10 that you may not know to be collecting.

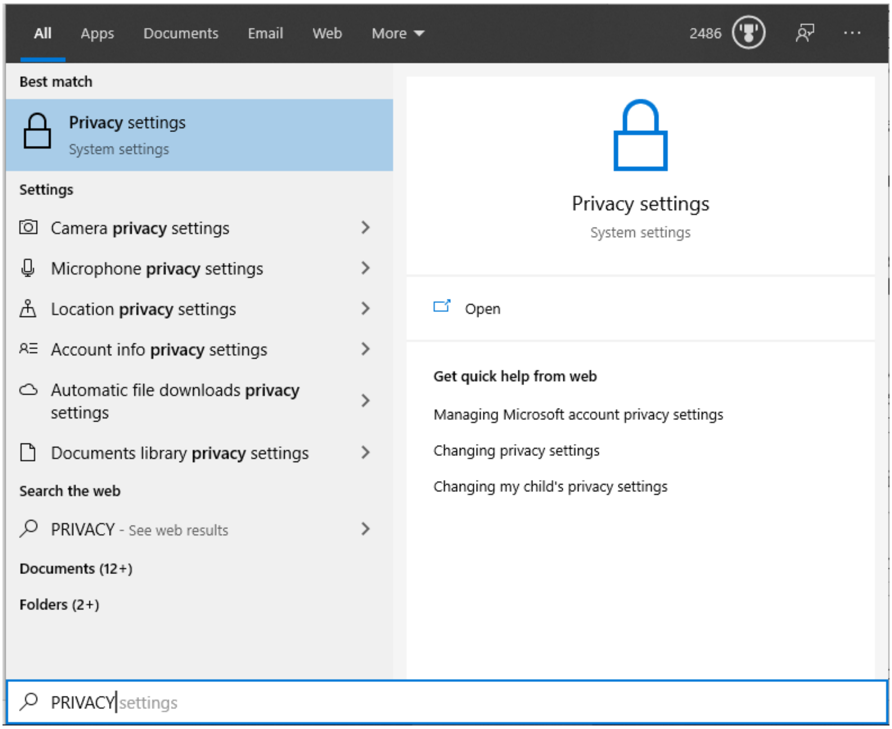
Whilst Yahoo, Twitter, Facebook and Google have been spying on their users for years, it was Microsoft's Windows 10 that seemingly copped most of the criticism on release.

Whilst Linux Operating Systems may be a better and safer bet, they are not entirely exempt from potential privacy violations and abandoning Windows or MacOS can be an incredibly disruptive solution for many users.

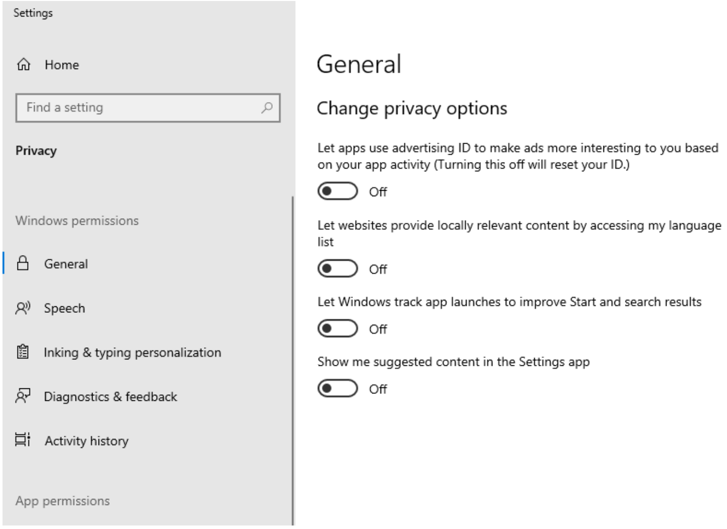
Windows Vista was Microsoft's first OS to collect diagnostic data. Whilst it was always assured that the data would help improve the quality of the Windows OS, it should be a concern as the product is not free. Any product that is offered for no cost at all will obviously cost in other ways but data collection to improve application compatibility, hardware and software issues involving Microsoft and third-party vendors is entirely the users choice – or at least it should be.

There are multiple “scheduled tasks” and embedded features such as requests for feedback or error reporting that can also disperse your data.

Your first step would be to visit and disable any permissions through the settings page. To do this navigate to the Privacy page by selecting START then SETTINGS and then PRIVACY or simply use the search function on the Start Menu.


All
Apps
Documents
Email
Web
More
2486
Best match
Privacy settings
System settings
Settings
Camera privacy settings
Microphone privacy settings
Location privacy settings
Account info privacy settings
Automatic file downloads privacy settings
Documents library privacy settings
Search the web
PRIVACY - See web results
Documents (12+)
Folders (2+)
Privacy settings
System settings
Open
Get quick help from web
Managing Microsoft account privacy settings
Changing privacy settings
Changing my child's privacy settings
PRIVACY settings

There will be a whole selection of Privacy Setting you can configure, but there's an easier option that is detailed below. On the PRIVACY SETTINGS page, be sure that your privacy options are configured as follows:



General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app activity (Turning this off will reset your ID.)

Off

Let websites provide locally relevant content by accessing my language list

Off

Let Windows track app launches to improve Start and search results

Off

Show me suggested content in the Settings app

Off

Furthermore, Windows 10 comes preinstalled with many applications you likely never use that also can collect data in the background. To easily select and remove any such applications and any data that is provided to Microsoft, Mirinsoft's Debotnet comes to your aid. It's 100% free for both personal and commercial use.

Debotnet:
https://www.mirinsoft.com/debotnet

There are multiple applications out there worth investigating that all do what Debotnet does, but some may offer better functionality or ensure that any new spy features are tackled. Every application suggested below is open-source. The reason only open-source software has been included is that it's more likely the project will be revised or taken over by another developer should it lack in updates:

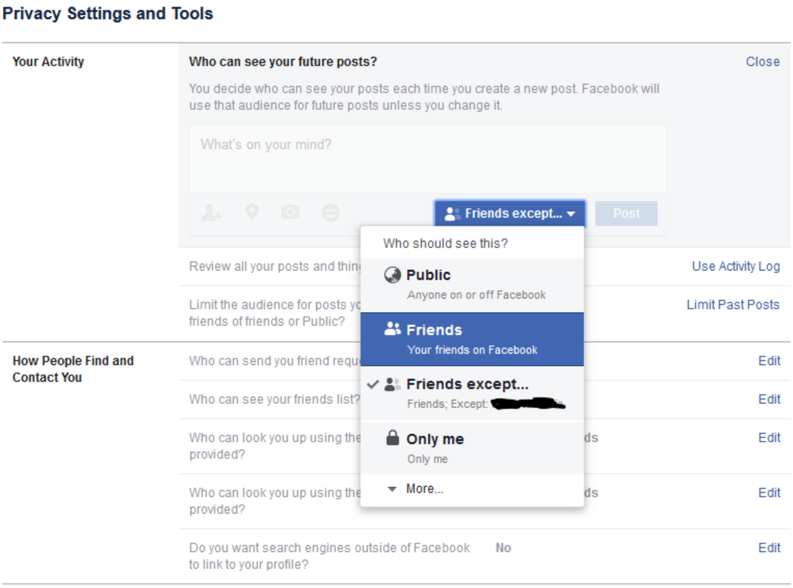
NAME	Features	URL
Debloat Windows 10	Disables telemetry, services and apps (mostly uses scripts rather than a graphical interface)	github.com/W4RH4WK/Debloat-Windows-10
PrivateWin10	Does everything plus has a custom firewall	github.com/DavidXanatos/priv10
DisableWinTracking	Easy to use and quickly allows you to choose what to disable	github.com/10se1ucgo/DisableWinTracking
Windows10Debloater	Various scripts including one that removes bloatware silently (great for custom installations)	github.com/Sycnex/Windows10Debloater
WindowsSpyBlocker	Another quick and easy application that disables various spy tactics and stats collection. Gives you the ability to go all-out and block every Microsoft update and application too	github.com/crazy-max/WindowsSpyBlocker

If you're not a Windows user, or you want to ditch Windows altogether then there are some handy comparisons at *https://www.privacytools.io/operating-systems*

SOCIAL MEDIA PRIVACY

FACEBOOK:

Limit access to your future posts to ensure that they are only visible to friends. This can reduce the about of data Facebook (and others) can collect from your browsing. To do this head to **Privacy Settings > Who can see your future posts?** then set it to **Friends** or you can even exclude specific people or create a group of people on Facebook you don't want to see your future posts.



Privacy Settings and Tools

Your Activity

Who can see your future posts? Close

You decide who can see your posts each time you create a new post. Facebook will use that audience for future posts unless you change it.

What's on your mind?

Friends except... ▾ Post

Who should see this?

- Public — Anyone on or off Facebook
- Friends — Your friends on Facebook
- ✓ Friends except... — Friends; Except: [redacted]
- Only me — Only me
- ▾ More...

Review all your posts and thin… — Use Activity Log

Limit the audience for posts y… friends of friends or Public? — Limit Past Posts

How People Find and Contact You

Who can send you friend requ… — Edit

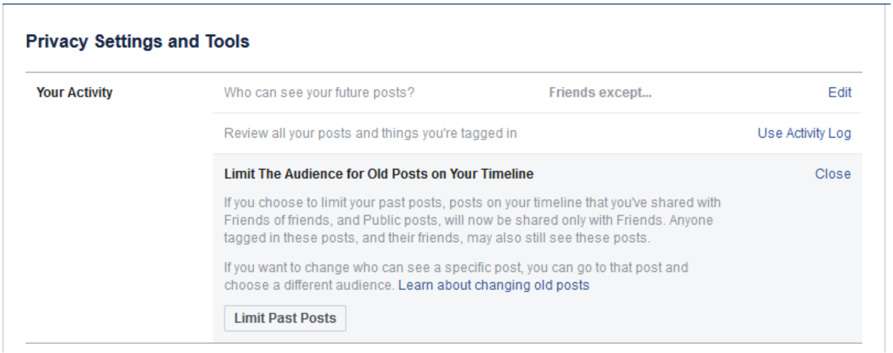
Who can see your friends list? — Edit

Who can look you up using the… provided? …ds — Edit

Who can look you up using the… provided? …ds — Edit

Do you want search engines outside of Facebook to link to your profile? No — Edit

You can also limit who can see your future posts. This is convenient for when you cringe at your own status updates from years before!



Privacy Settings and Tools

Your Activity

Who can see your future posts? Friends except... Edit

Review all your posts and things you're tagged in Use Activity Log

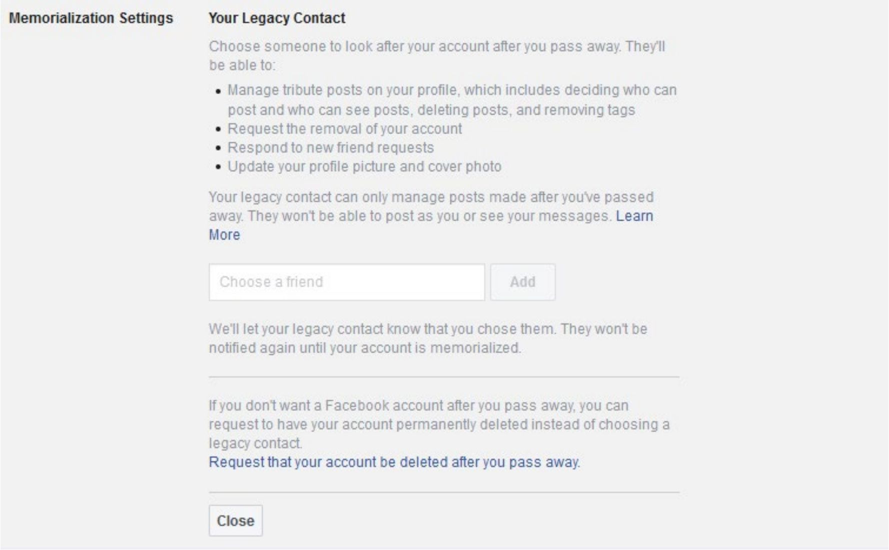
Limit The Audience for Old Posts on Your Timeline Close

If you choose to limit your past posts, posts on your timeline that you've shared with Friends of friends, and Public posts, will now be shared only with Friends. Anyone tagged in these posts, and their friends, may also still see these posts.

If you want to change who can see a specific post, you can go to that post and choose a different audience. Learn about changing old posts

It's a rather horrible thing to have to set up, but you can also decide what happens to your Facebook account when you pass away.

This is achieved in the **General Account Settings** section **Memorialization Settings**:



Memorialization Settings

Your Legacy Contact

Choose someone to look after your account after you pass away. They'll be able to:

- Manage tribute posts on your profile, which includes deciding who can post and who can see posts, deleting posts, and removing tags
- Request the removal of your account
- Respond to new friend requests
- Update your profile picture and cover photo

Your legacy contact can only manage posts made after you've passed away. They won't be able to post as you or see your messages. Learn More

We'll let your legacy contact know that you chose them. They won't be notified again until your account is memorialized.

If you don't want a Facebook account after you pass away, you can request to have your account permanently deleted instead of choosing a legacy contact.

Request that your account be deleted after you pass away.

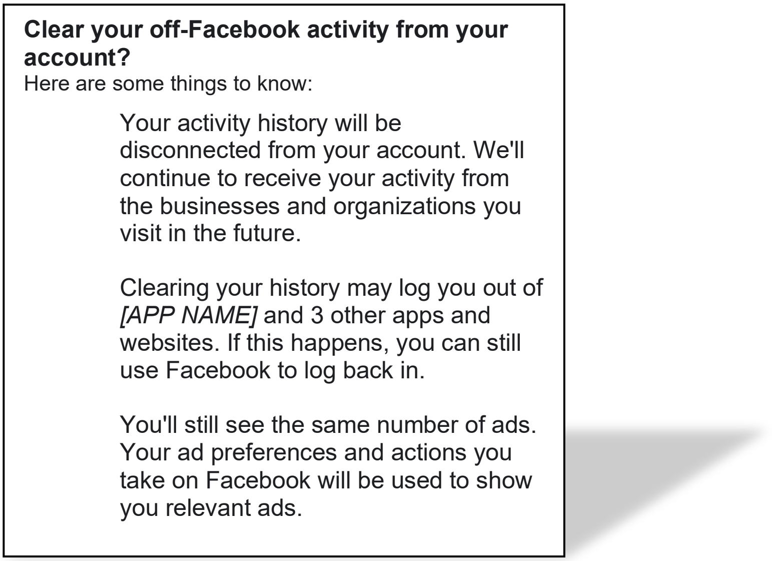
After the Cambridge Analytica scandal, Facebook launched a feature within user controls called “Off-Facebook Activity”. According to the Facebook page:

> *Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them. Interactions are things like visiting their website or logging into their app with Facebook. Off-Facebook activity does not include customer lists that businesses use to show a unique group of customers relevant ads.*

Within the Off-Facebook Activity page featured a variety of information relating to what advertisers and had stored. Alongside this information would be the function to download GDPR-Compliant data exports and a “Your Information” section that gives users an online repository of data that is collected and stored in Facebook’s servers.

Facebook claims it uses data to suggest groups, marketplace items and businesses the user may be interested in.

Choosing to clear any of the Off-Facebook Activity presents the user with this warning:



Clear your off-Facebook activity from your account?

Here are some things to know:

Your activity history will be disconnected from your account. We'll continue to receive your activity from the businesses and organizations you visit in the future.

Clearing your history may log you out of *[APP NAME]* and 3 other apps and websites. If this happens, you can still use Facebook to log back in.

You'll still see the same number of ads. Your ad preferences and actions you take on Facebook will be used to show you relevant ads.

Much-like Googles' similar feature, Takeout, the "Information About You" archive contains multiple directories that feature various cleanly-presented lists of things that Facebook has stored on the user. The "interests" list is an extensive log of any pages the user has "liked" or commented on. The "Off-Facebook Information" section is comprised of mainly third-party applications and services the user has connected to their accounts through sign-in or linked profiles.
Many of the "Advertisers and Businesses" included in the "who have uploaded and shared a list with your info" tend to be entirely unrelated to the interests of the user. Furthermore, any information permitted to third-party advertisers such as relationship status and employment status can be connected to provide the user with targeted advertisements. For example, allowing ads that are "intended to reach people based on these profile fields" can show dating websites and employment offers if one is listed as single and unemployed.

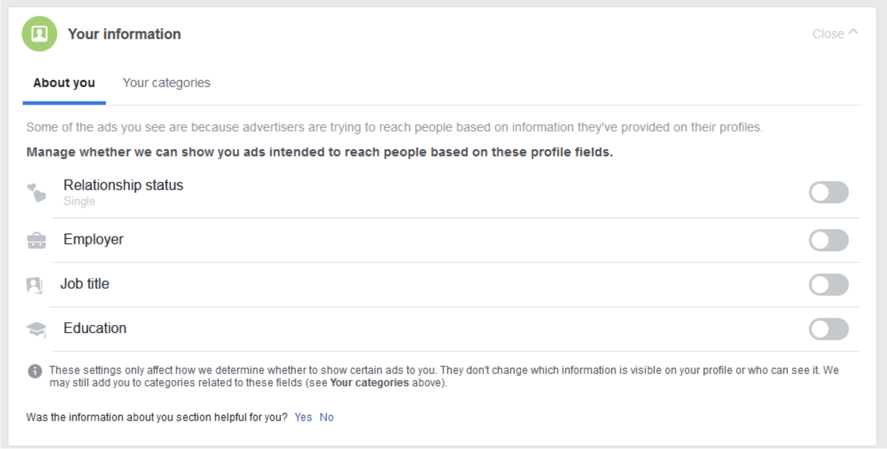
Clearing search history and not enabling advertisers to see profile fields and information is an advisable method of maintaining your privacy should you wish to use Facebook.

The clear history tool can be accessed by following these directions:

On your desktop:
Settings > Your Facebook Information > A section titled "Off-Facebook Activity" will appear. Click on the "View" link next to it.

On your Mobile:

Menu > Settings and Privacy > Settings > scroll down to the "Your Facebook Information" field and tap "Off-Facebook Activity" to view and modify this information.



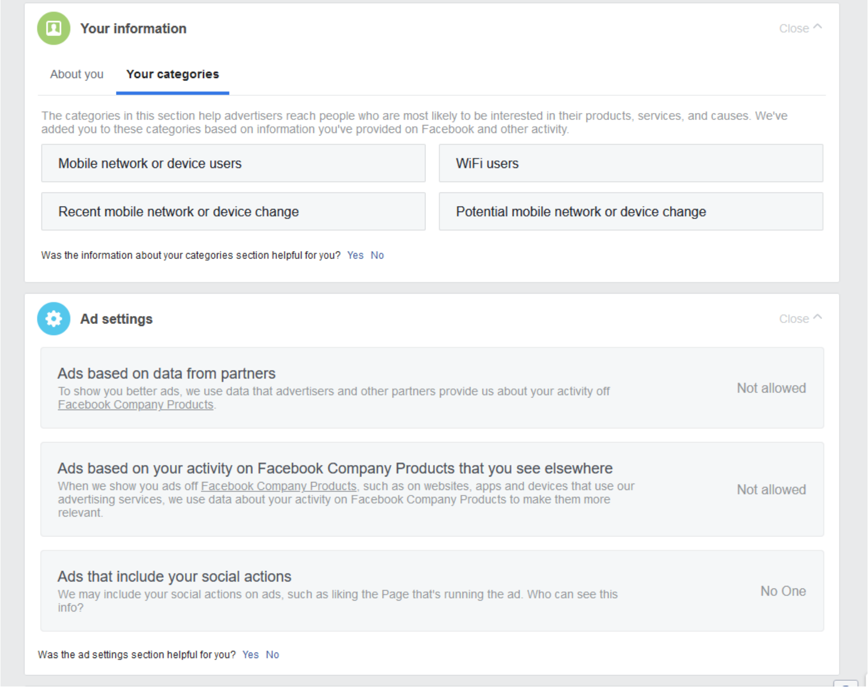
Some of the ads you see are because advertisers are trying to reach people based on information they've provided on their profiles.

Manage whether we can show you ads intended to reach people based on these profile fields.

- Relationship status
Single
- Employer
- Job title
- Education

These settings only affect how we determine whether to show certain ads to you. They don't change which information is visible on your profile or who can see it. We may still add you to categories related to these fields (see **Your categories** above).

Was the information about you section helpful for you? Yes No



The categories in this section help advertisers reach people who are most likely to be interested in their products, services, and causes. We've added you to these categories based on information you've provided on Facebook and other activity.

Mobile network or device users	WiFi users
Recent mobile network or device change	Potential mobile network or device change

Was the information about your categories section helpful for you? Yes No

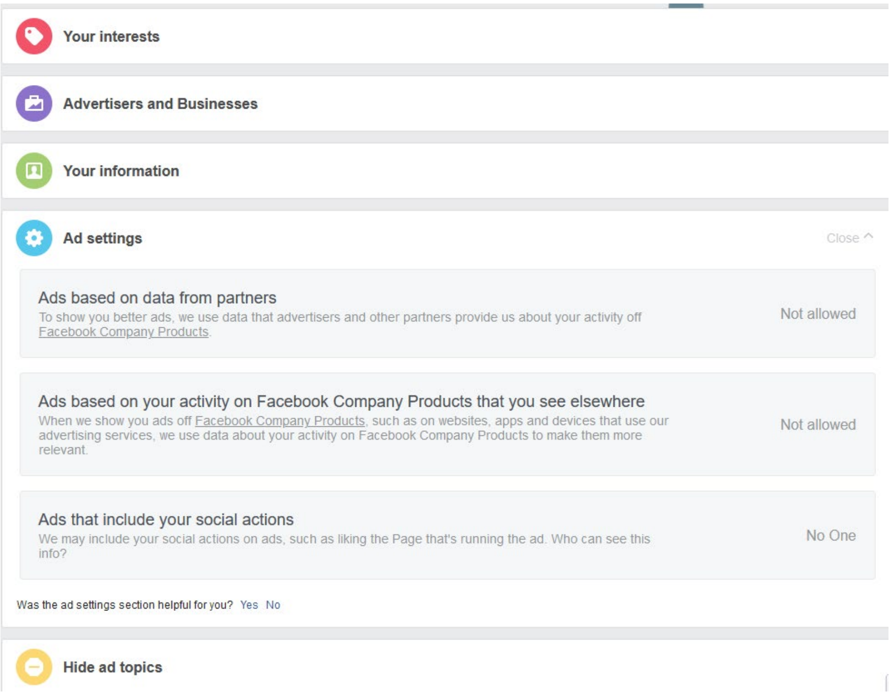
Ads based on data from partners
To show you better ads, we use data that advertisers and other partners provide us about your activity off Facebook Company Products.
Not allowed

Ads based on your activity on Facebook Company Products that you see elsewhere
When we show you ads off Facebook Company Products, such as on websites, apps and devices that use our advertising services, we use data about your activity on Facebook Company Products to make them more relevant.
Not allowed

Ads that include your social actions
We may include your social actions on ads, such as liking the Page that's running the ad. Who can see this info?
No One

Was the ad settings section helpful for you? Yes No

In the settings area you can also choose **Ads** which will allow you to gain a little more control over the ads you see, and your Facebook usage being linked with relevant ads:



Your interests

Advertisers and Businesses

Your information

Ad settings

Close

Ads based on data from partners
To show you better ads, we use data that advertisers and other partners provide us about your activity off Facebook Company Products.

Not allowed

Ads based on your activity on Facebook Company Products that you see elsewhere
When we show you ads off Facebook Company Products, such as on websites, apps and devices that use our advertising services, we use data about your activity on Facebook Company Products to make them more relevant.

Not allowed

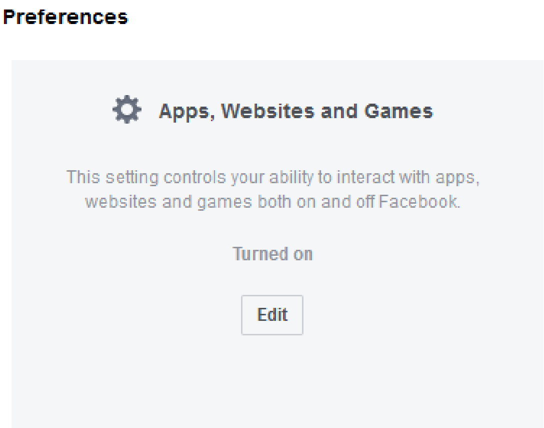
Ads that include your social actions
We may include your social actions on ads, such as liking the Page that's running the ad. Who can see this info?

No One

Was the ad settings section helpful for you? Yes No

Hide ad topics

Under **Apps and Websites** you can see if there are any connected applications that you may no longer use or want connected to your account:



Preferences

Apps, Websites and Games

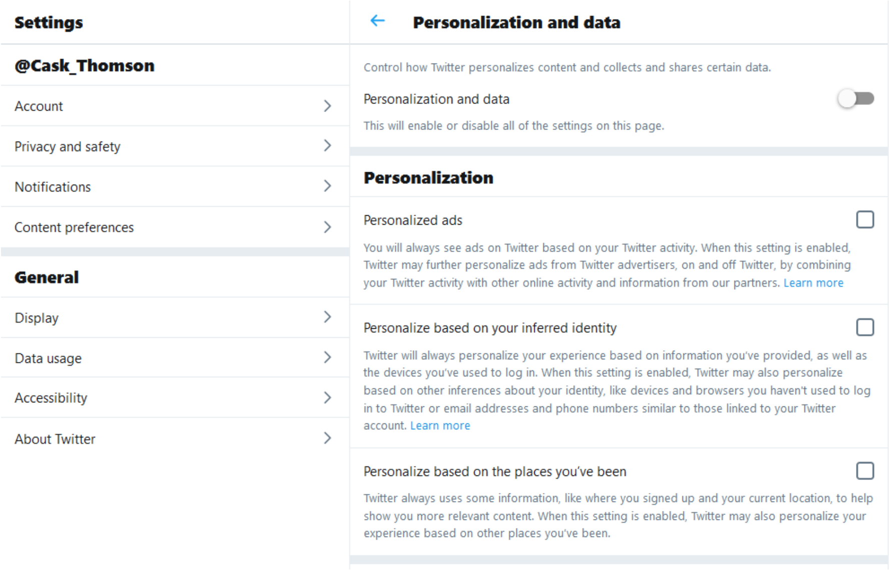
This setting controls your ability to interact with apps, websites and games both on and off Facebook.

Turned on

Edit

TWITTER:

In your settings you can delete all location history and disable all personalisation and data.



Personalization and data

Control how Twitter personalizes content and collects and shares certain data.

Personalization and data ○

This will enable or disable all of the settings on this page.

Personalization

Personalized ads □

You will always see ads on Twitter based on your Twitter activity. When this setting is enabled, Twitter may further personalize ads from Twitter advertisers, on and off Twitter, by combining your Twitter activity with other online activity and information from our partners. Learn more

Personalize based on your inferred identity □

Twitter will always personalize your experience based on information you've provided, as well as the devices you've used to log in. When this setting is enabled, Twitter may also personalize based on other inferences about your identity, like devices and browsers you haven't used to log in to Twitter or email addresses and phone numbers similar to those linked to your Twitter account. Learn more

Personalize based on the places you've been □

Twitter always uses some information, like where you signed up and your current location, to help show you more relevant content. When this setting is enabled, Twitter may also personalize your experience based on other places you've been.

MOBILE DEVICE PRIVACY

If you're an Android user, then Google has many applications and services that are embedded into the Operating System. These are usually filled with tricky data collection methods. The best way to have a pure freedom-filled Android mobile phone or device is to ***root*** (in simple terms, unlocking the device if required) your phone and install a clean Android distribution such as LineageOS[1]

LineageOS is a free, open-source operating system for phones, tablet devices and even home entertainment media devices. The main issue with installing a custom Android distribution is the lack of compatibility with many phones. If you're shopping for an Android device that you can use specifically for LineageOS then your best bet is to view the devices that are confirmed as having little issue and has documentation on the LineageOS Wiki on installation.[2] More information on a variety of devices can be found at the XDA Developers forum[3] which has been involved in the development and discussion of software and hardware modifications since 2002.

Whilst LineageOS isn't the only available option, it is one of the most supported with plenty of available information.

This doesn't mean you are still locked into using Google applications across your Android device. For example, you can use F-Droid[4] to download many applications that are unavailable or banned from Google Play such as advertisement blockers and YouTube video downloaders that Google prohibits from being released via their app store.

[1] https://lineageos.org/

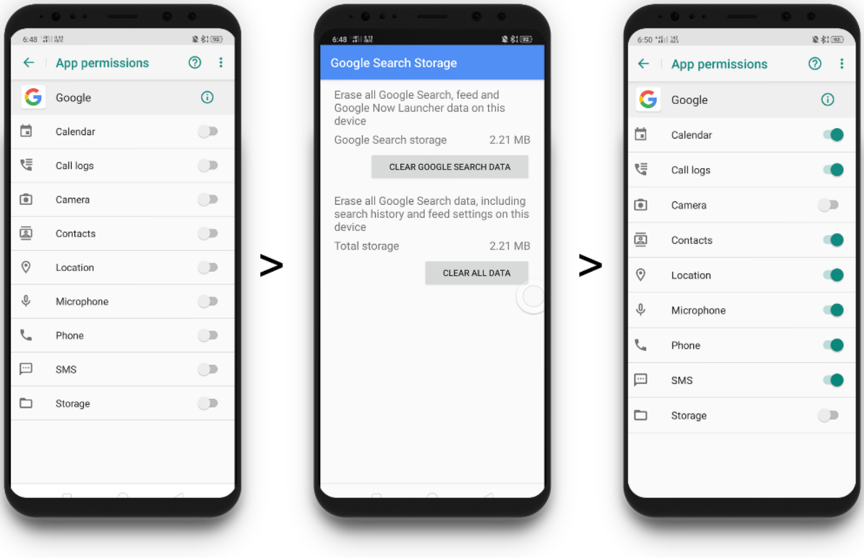
[2] https://download.lineageos.org/

[3] https://forum.xda-developers.com

[4] https://f-droid.org/

As for the particular Google (and other) services, be sure to take a look at the screens below which can be accessed via the Settings menu.

Whenever you clear data, the settings are reverted to default, so be sure to keep an eye on that. For instance, clearing Google search data can cause App Permissions to revert to their previous values:



6:48

App permissions

Google

- Calendar ○
- Call logs ○
- Camera ○
- Contacts ○
- Location ○
- Microphone ○
- Phone ○
- SMS ○
- Storage ○

>

6:48

Google Search Storage

Erase all Google Search, feed and Google Now Launcher data on this device

Google Search storage 2.21 MB

CLEAR GOOGLE SEARCH DATA

Erase all Google Search data, including search history and feed settings on this device

Total storage 2.21 MB

CLEAR ALL DATA

>

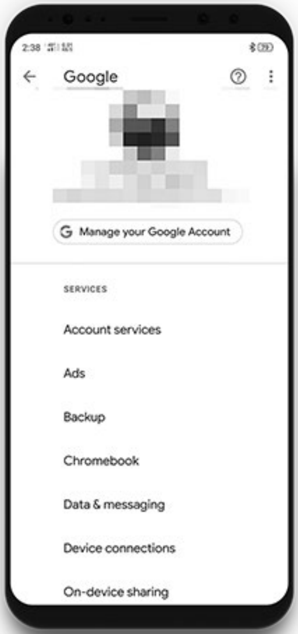
6:50

App permissions

Google

- Calendar ●
- Call logs ●
- Camera ○
- Contacts ●
- Location ●
- Microphone ●
- Phone ●
- SMS ●
- Storage ○

Here are some other settings and permissions you may also want to look at:



Google

Manage your Google Account

SERVICES

Account services

Ads

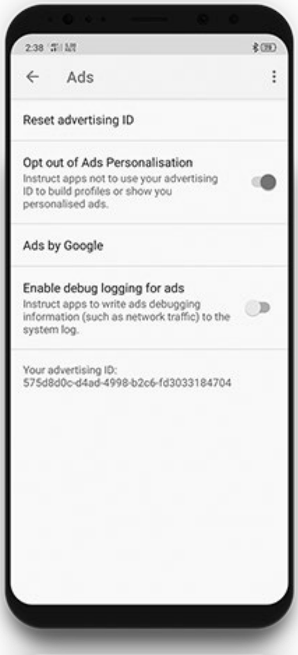
Backup

Chromebook

Data & messaging

Device connections

On-device sharing



Ads

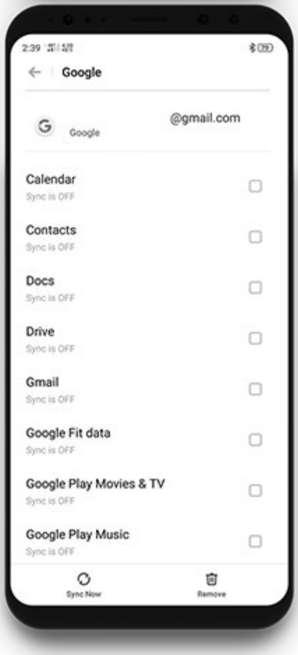
Reset advertising ID

Opt out of Ads Personalisation
Instruct apps not to use your advertising ID to build profiles or show you personalised ads.

Ads by Google

Enable debug logging for ads
Instruct apps to write ads debugging information (such as network traffic) to the system log.

Your advertising ID:
575d8d0c-d4ad-4998-b2c6-fd3033184704



Google

@gmail.com
Google

Calendar □
Sync is OFF

Contacts □
Sync is OFF

Docs □
Sync is OFF

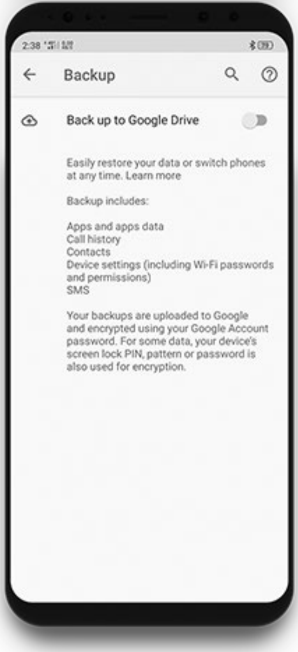
Drive □
Sync is OFF

Gmail □
Sync is OFF

Google Fit data □
Sync is OFF

Google Play Movies & TV □
Sync is OFF

Google Play Music □
Sync is OFF



Backup

Back up to Google Drive

Easily restore your data or switch phones at any time. Learn more

Backup includes:

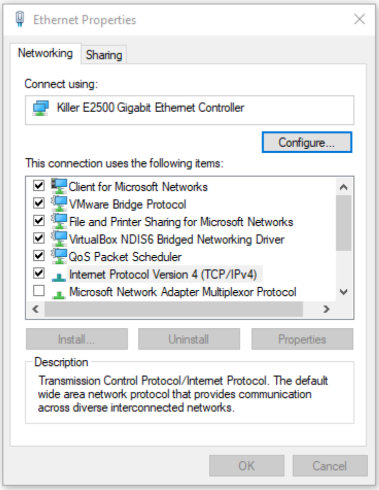
Apps and apps data
Call history
Contacts
Device settings (including Wi-Fi passwords and permissions)
SMS

Your backups are uploaded to Google and encrypted using your Google Account password. For some data, your device's screen lock PIN, pattern or password is also used for encryption.

PROTECTING YOUR COMPUTER AND INTERNET WITH BLOCKLISTS AND HOSTS:

Your computer and modem are configured to use Domain Name System (DNS) numbers. Without going to deep into what these numbers do and the benefits of using DNS settings that are set by you and not your ISP, here are some basic methods to change your DNS and the benefit of doing so. Whilst most decentralised public DNS servers are free, premium options also exist and can provide faster and more-secure results. When using public DNS, all *lookups* are done through the servers owned by the provider. For example, Google's Public DNS server utilises Google's servers to increase speeds and provide better reliability than ISP-powered ones.

Google's Public DNS uses the numbers. To activate, one would configure their network settings on either their computer or modem (or both) to use the IP addresses 8.8.8.8 and 8.8.4.4 like so:



Ethernet Properties

Networking | Sharing

Connect using:

Killer E2500 Gigabit Ethernet Controller

Configure...

This connection uses the following items:

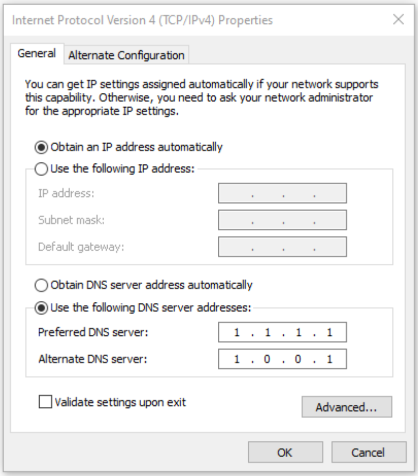
- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ VirtualBox NDIS6 Bridged Networking Driver
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 1 . 1 . 1 . 1

Alternate DNS server: 1 . 0 . 0 . 1

☐ Validate settings upon exit

Advanced...

OK | Cancel

The example shows a Windows operating system, but as each OS varies, it's best to check with the provider how to configure DNS on your mobile phone, OS or modem. For a book that has spent many chapters criticising Google, you will notice that the 8.8.8.8 and 8.8.4.4 DNS servers are not configured on the screenshot. Instead, the free public DNS numbers 1.1.1.1 and 1.0.0.1 are displayed. These numbers are provided by Cloudflare, a Content Delivery Network (CDN) who do not sell the data of users taking advantage of their free Public DNS. According to global traffic management provider PerfOps' service DNSPerf[5], 1.1.1.1 is often the fastest available DNS server with a reliable network performance.

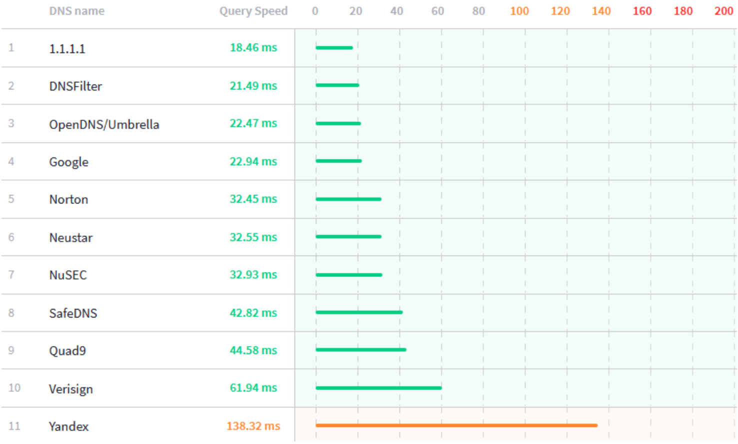
[5] https://www.dnsperf.com/#!dns-resolvers

The website's benchmarks showcase Google, Verisign and Norton's servers as being a very slight percentage more reliable in overall uptime but as one of the primary secure providers, Cloudflare's DNS names have had fairly consistent results worldwide next to OpenDNS/Umbrella, DNSFilter, Google and SafeDNS to name but a few.
Morally, however, you may disagree with Cloudflare's stance on specific cases of censorship as detailed in Part Three.

Simply changing your DNS can also bypass many internet filters set by ISPs. For example, many of the blocks by Australian and New Zealand providers during terror events mentioned previously in the book could and can be circumvented using different DNS servers. Many ISPs filtering copyright infringing content use blocks at a DNS level also.

Premium DNS providers often offer the ability to choose the location of servers used. For example, OpenDNS – which is owned by American networking technology company Cisco – give 'business' users the option to select the locale of the server they wish to use for speed and security purposes.

Many DNS providers also provide users with additional security by blocking websites that are known to raise security concerns such as websites that impersonate popular companies in order to steal password data (often referred to as phishing) and many services allow users to register and choose to block access to sites that feature pornography, gambling or other content a user may wish to prevent from being accessed by internet users on their network. Some providers, such as AdGuard, specialise in the blocking of advertising networks at a network-level for users who do not wish to install extensions suggested within the chapter.



	DNS name	Query Speed
1	1.1.1.1	18.46 ms
2	DNSFilter	21.49 ms
3	OpenDNS/Umbrella	22.47 ms
4	Google	22.94 ms
5	Norton	32.45 ms
6	Neustar	32.55 ms
7	NuSEC	32.93 ms
8	SafeDNS	42.82 ms
9	Quad9	44.58 ms
10	Verisign	61.94 ms
11	Yandex	138.32 ms

Results of the most popular free Public DNS services measured (Less is better)

As with many online service providers, Public DNS providers should be researched if you are concerned that the claims of privacy and not selling user data are incorrect. A majority of major services specify exactly what they do and do not collect in their Privacy Policies or Privacy Notices. Many of these companies offer a premium service and provide a free one to encourage users to consider their business or commercial products. Whilst companies like Google claim to ‘temporarily store’ data collected through the use of Google Public DNS, the short privacy policy makes it clear that some data is retained:

> *In the permanent logs, we don't keep personally identifiable information or IP information. We do keep some location information (at the city/metro level) so that we can conduct debugging, analyze abuse phenomena.* ***After keeping this data for two weeks, we randomly sample a small subset for permanent storage.***

The next page contains a list of popular free public DNS providers and the addresses (numbers)

The list is in no particular order and have been verified as safe. As always, it is recommended you research each company before choosing to use them.

As of book publication, the providers listed do not collect personally identifiable data and do not collect data for the purpose of sale.

The first address is the primary (or preferred) and the second the alternate.

In some cases, there are four addresses. These relate to ‘family’ filtered DNS resolvers which block content such as pornography. The third and fourth lines are the primary and alternate addresses, respectively

Provider	IPv4 Addresses	Ipv6 Addresses	Comments
Quad9 [second set of addresses are unfiltered **do not** block malicious sites]	9.9.9.9 149.112.112.112 9.9.9.10 149.112.112.10	2620:fe::fe 2620:fe::9 2620:fe::10 2620:fe::fe:10	Only blocks domains known to be associated with malicious activity. Non-profit organisation.
AdGuard	*176.103.130.130* *176.103.130.131* *176.103.130.132* *176.103.130.134*	*2a00:5a60::ad1:0ff* *2a00:5a60::ad2:0ff* *2a00:5a60::bad1:0ff* *2a00:5a60::bad2:0ff*	*Privacy-oriented system that blocks tracking, ads and malicious attacks.*
Cloudflare	1.1.1.1 1.0.0.1	*2606:4700:4700::1111* *2606:4700:4700::1001*	
Google	8.8.8.8 8.8.4.4	2001:4860:4860::8888 2001:4860:4860::8844	Stores logs and collects analytics. Book has failed if you use these names.
Verisign	64.6.64.6 64.6.65.6	2620:74:1b::1:1 2620:74:1c::2:2	
CleanBrowsing	185.228.168.168 185.228.169.168	2a0d:2a00:1:: 2a0d:2a00:2::	Heavily filtered, Designed for safe use by children under 13
OpenNIC	185.121.177.177 169.239.202.202	2a05:dfc7:5::53 2a05:dfc7:5::5353	User-owned and user-controlled. “Tier2” servers listed on website are provided by verified volunteers regionally.

Note: Using one of the many OpenNIC servers gives you access to multiple unlisted websites utilising exclusive domain names that can’t be reached by those outside of the OpenNIC Public DNS. Servers are provided by volunteers, so it is best to see https://www.opennic.org/ to discover your closest.

HOSTS FILES

Almost every operating system utilises a user-editable text file that contains hostnames and addresses of hosts to block and prevent specified applications from accessing the internet. Several websites dedicated to maintaining a list of host files or entries to insert exist, with many security organisations providing extensive lists of websites reported by software or users as a threat to the security of their computer and network. Anti-Virus and Firewall applications often incorporate these lists within their software, but computer and mobile device users can easily edit their own hosts files with minimal risk. Many of the lists provided by user-collaborative websites are compatible with standard OS hosts files, blacklists/blocklists or as data files that can be used with P2P (Peer-to-Peer) applications. Websites such as iblocklist[6] provide lists that relate to categorical blocking such as blocking government tracking, known paedophilia websites and tracking by software applications or companies such as Google and Microsoft. These lists are often free to download with more up-to-date lists provided for subscribed users. Another popular and frequently updated hosts file for Windows users is the MVPS Hosts file[7] which has been maintained since 1998.

The hosts file for modern Windows operating systems (including XP, 2003, Vista, 2008, 7, 8 and 10) is located at `C:\Windows\System32\drivers\etc`

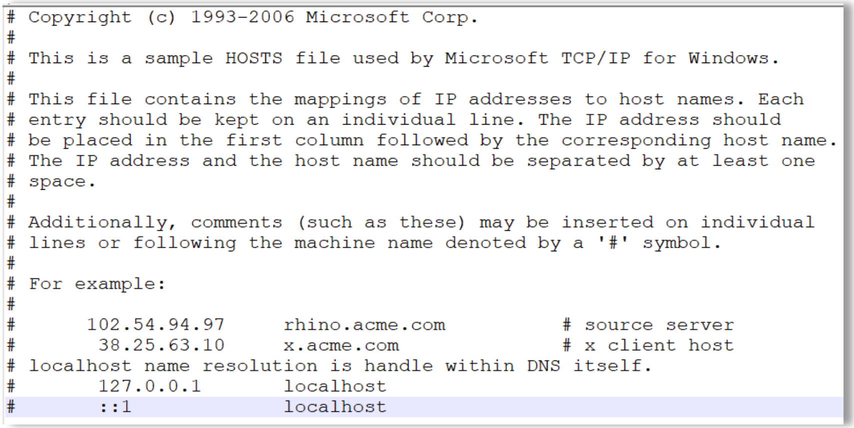
[6] https://www.iblocklist.com/

[7] https://winhelp2002.mvps.org/hosts.htm

Mac OS X 10.0 to 10.1.5 users can edit hostes through NetInfo or niload whilst Mac OS X 10.2 and later users can find hosts files at `/etc/hosts` whilst Android, iOS and Linux users can also edit the file at this location. Linux users can also use a terminal-based text editor such as nano to edit the file by typing the command:

```
sudo nano /etc/hosts
```

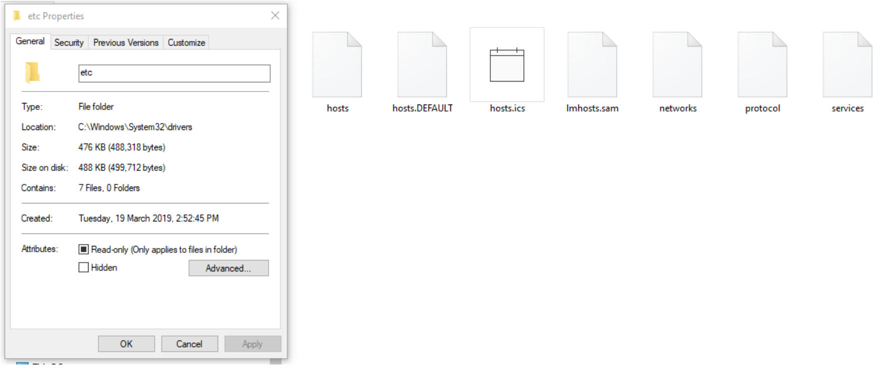
The default Windows hosts file is made up of instructions for editing:



```
# Copyright (c) 1993-2006 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handle within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

Each # is a comment and the final line is the end of the default file. Comments can be added and removed without affecting the list. A hosts file contains no file extension, and therefore should be renamed to hosts.txt in order to edit with Notepad. It's advisable to create a copy of your hosts file before editing should there be any mistakes. Renaming the file hosts.bak OR hosts.default will allow you to revert any changes by simply removing the incorrect hosts file and returning the original name "hosts"

As seen in the next screenshot, I have named the very original unedited hosts file of a fresh Windows 10 installation "hosts.DEFAULT"



etc

Type: File folder
Location: C:\Windows\System32\drivers
Size: 476 KB (488,318 bytes)
Size on disk: 488 KB (499,712 bytes)
Contains: 7 Files, 0 Folders

Created: Tuesday, 19 March 2019, 2:52:45 PM

Attributes: ☒ Read-only (Only applies to files in folder)
□ Hidden

You can add any website for whatever reason by entering a new line and typing 127.0.0.1 and the URL you wish for all applications to block. For example, the following entries would block anything that comes from Facebook.com and Google.com:

```
127.0.0.1 https://facebook.com
127.0.0.1 https://google.com
```

Take note that above example will block the ***https://*** URL but not the standard ***http://*** and therefore you would be required to add both entries, or block the websites by entering just the domain name such by entering ***127.0.0.1 google.com*** Hosts files are also useful for blocking application activations and are commonly used to patch . Don't forget the importance of a good password. The GitHub repository[8] SecLists, operated by members of the Open Web Application Security Project (OWASP), showcases many of the most-breached passwords and usernames found across the internet; some of which are purchasable through the Dark Web which is explored in the next chapter.

[8] https://github.com/danielmiessler/SecLists

Software such as the handy extension uBlock, suggested previously, use a similar system of text lists to filter out any advertisements and privacy risks. Many of these lists are maintained or verified by Easiest[9] who frequently provide a number of different lists depending on personal preferences. This can include the blocking of online advertisements to the complete blocking of Facebook connections or even connections that relate to countries and their respective governments and businesses a user may not trust. Some such lists such as *Annoyance* filters[10] simply attempt make your online experience better by preventing sign-up requests, invitations for you to sign-up for a website's mailing list or the irritating GDPR compliance notices that have appeared throughout the internet since the European Union's regulations came into effect.

Before activating any filters or adding thousands of entries in your hosts file from community lists, you may want to do a quick check to see if any of the websites you frequent will be blocked. For example, the StevenBlack unified lists[11] on GitHub are fantastic and are categorised to give you control over whether you are blocking adware and malware, pornography, fake news or all of the above but some entries are disagreeable. For example, the definition of fake news is objective and many websites you may read could be included in these lists. As the creator of one Fake News hosts list states[12] *"the term [fake news] quickly became adopted by many to simply mean* ***news I don't agree with."***

[9] https://easylist.to/

[10] https://forums.lanik.us/

[11] https://github.com/StevenBlack/hosts

[12] https://github.com/marktron/fakenews

Another, though somewhat complex, option is to set up a hardware filter to block dodgy websites across your network. Essentially, you can be your own censorship dictator by building a dedicated network routing device – and it's a lot less expensive than you might think. Free open source solutions like OpenWrt (Open ***W***ireless ***R***ou**T**er) can be run on routers, wireless modems, smartphones or even an old laptop or desktop computer you may have lying around (though obviously power usage and size would need to be considered)
Another option is to use the minicomputer Raspberry Pi which is an extremely cheap but powerful computer by a UK charity encouraging learning and computer science education. The Pi has multiple attachments available too such as internal touch screens and almost endless options for casing the little unit. Dedicated solutions like Pi-hole are fantastic for blocking advertisements and keeping your network safe.
More details on the the Pi are explored soon in ***Be Your Own Cloud***.
Both options are suggested purely due to the huge trove of information available online.

OpenWrt:
https://openwrt.org/
https://openwrt.org/toh/start
https://openwrt.org/faq/which_router_should_i_buy

Pi-Hole:
https://pi-hole.net/
https://www.raspberrypi.org/

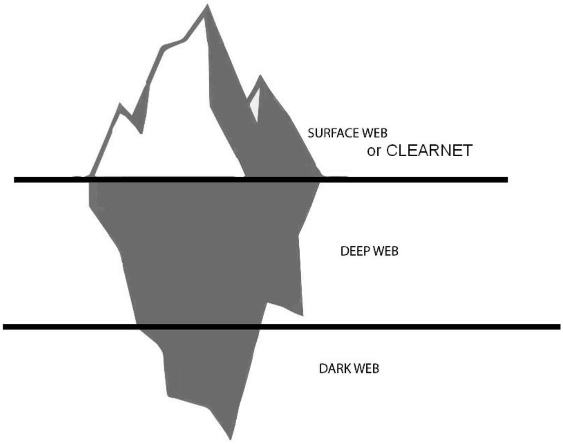
More locations to find entries to create your own ultimate hosts file:
https://someonewhocares.org/hosts/
https://www.hostsfile.org/hosts.html
https://www.malwaredomainlist.com/

THE DEPTHS OF THE INTERNET

Although the terms Deep Web and Dark Web are thrown around by various media outlets; the two are not the same thing. Deep Web refers to anything on the internet that is not indexed by a search engine or made publicly visible to users. This could mean any website that requires a password or payment, or an online dashboard intended to be accessed only by employees of a business. Deep Web can also refer to websites that are only accessible to those invited to register. The internet is typically described as an iceberg with the 'surface' of the iceberg being the common web that most of us use on a day-to-day basis.

The Dark Web, on the other hand, is a division of the Deep Web that is intentionally hidden and requires specific tools such as Tor to access. This chapter will cover how and why one may want to access this depth of the internet.

The **Dark Web** is the deepest layer of the iceberg containing black market sites, counterfeit and fraudulent content, whistle-blower content and leaks, various legal and illegal or objectionable pornography and various online anonymous services offering anything from databases of password leaks to drugs and severe crimes. Whilst many sites found on the Dark Web contain genuinely criminal content and claim to showcase top-secret experiments conducted in underground labs by the authors – some even with photographs of evidence – a majority of these sites have proven to be the work of hoaxers intending to shock visitors and journalists. With such anonymity, it's hard to know what is and isn't real on the internet; but the Dark Web can take it one step further. Enter at your own risk and remember not all is what it seems. Many websites accessible only via the Dark Web are intentionally ominous and filled with false information.



As for the security of you and your devices; everything is always 99%. You may not be truly protected using the options detailed in this chapter. Care must always be taken to ensure that any potential spying devices such as cameras, microphones and components that may possibly bypass inbuilt security features are completely disconnected. This can involve simply taping over an inbuilt camera or using an operating system like Tails (detailed later) that is developed with accessing the Dark Web in mind.

Always disable JavaScript and never expand the browser window to full as this can help identify the user.

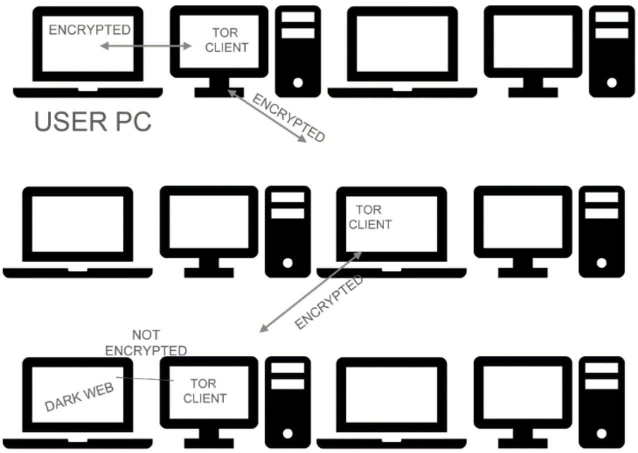
Virtual Private Networks (VPNs) are great for various reasons such as tricking a website into thinking you're accessing it from another location or trying to bypass a website that has been blocked by the government or a company in your country, VPNs are not anonymous and should not be used as a sole method of protecting yourself online. VPN providers are able to view all traffic and any sites you have accessed. VPNs are susceptible to hackers. Anyone who successfully hacks into a VPN server can gain control of the server and retrieve data stored within. Authorities are also able to serve VPN providers with court orders to see any history they believe may be linked to your account and online activity. As described within this book; many countries have laws in-place that give easy access to any power seeking to subpoena any company providing an online service.

TOR AND .ONION

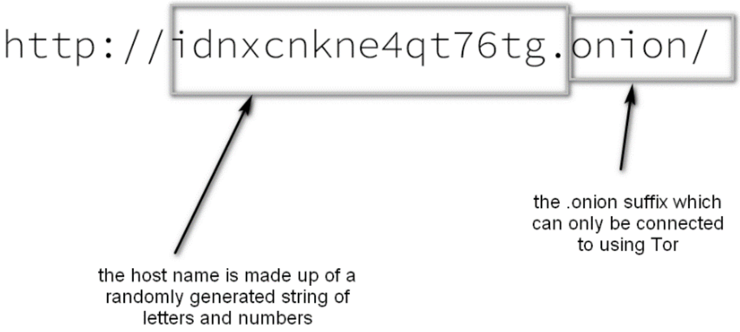
Tor is the largest, most robust, and most effective metadata-resistant software project. Known also as The Onion Router, Tor is optimised for low-latency web browsing with the intention of providing an access point for websites that cannot be accessed using normal web browsers. Many large-scale websites such as Wikipedia block editing from those using Tor. Some websites even block access altogether. As one should expect, Tor does not offer certain anonymity.

In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion. The encrypted data is transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

The diagram below is a simplistic explanation of how Tor works. Tor uses a worldwide network that consists of thousands of volunteers and relays that conceal the users' location. The users' chosen Tor client picks a random path to reach the destination server. This can be a painfully slow process, resulting in many sites of the Dark Web being minimal in rich content.



Websites accessible only via the Tor network have the domain extension ***.onion.*** This suffix is considered a 'special use domain' by overseers Internet Corporation for Assigned Names and Numbers (ICANN), Internet Assigned Numbers Authority (IANA) and Internet Engineering Task Force (IETF) respectively. Below is an example of an Onion URL:

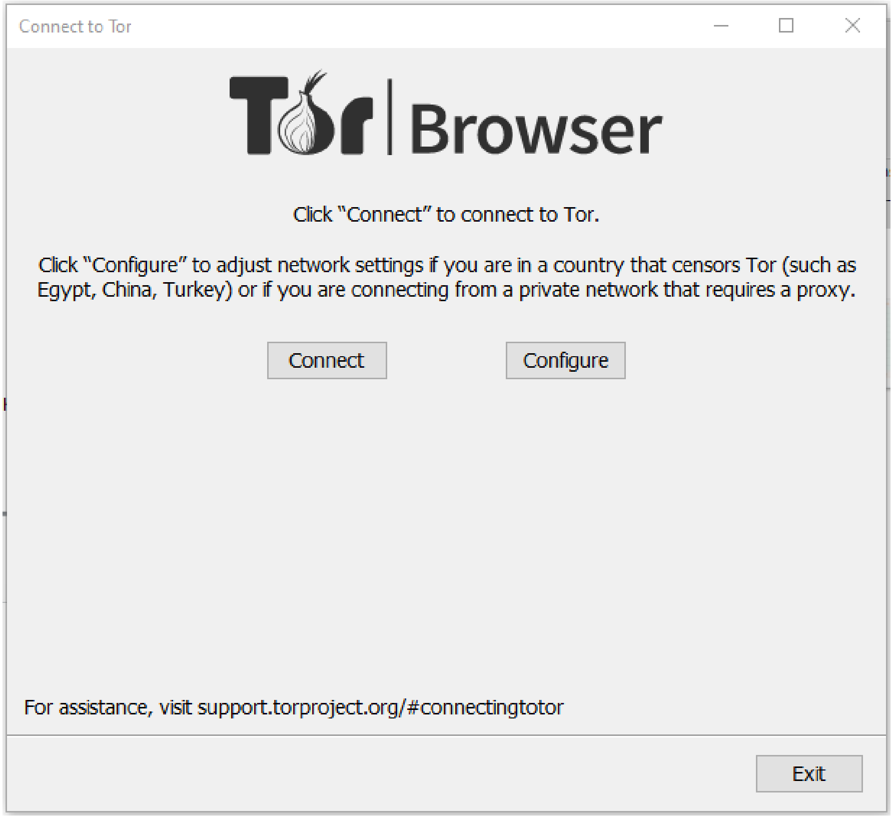

http://idnxcnkne4qt76tg.onion/
the host name is made up of a randomly generated string of letters and numbers
the .onion suffix which can only be connected to using Tor

(Accessing the link above will likely result in error, as it is the old link to access search engine DuckDuckGo)

As explained before, there are two ways to access the Tor anonymity network. The first one is less secure and involves simply running the purpose-built browser from your desktop computer. The second way involves installing a ‘live’ operating system that can be run from a USB drive. Should you be physically caught or feel compromised whilst using this USB drive, you can pull it out and it will shut down and clear all data associated with it.

Installing Tor browser is pretty simple:
Head to *https://www.torproject.org/download/*
One downloaded, you can install the browser in any folder of your choosing.

Launch the Tor application and you'll be given the following window:



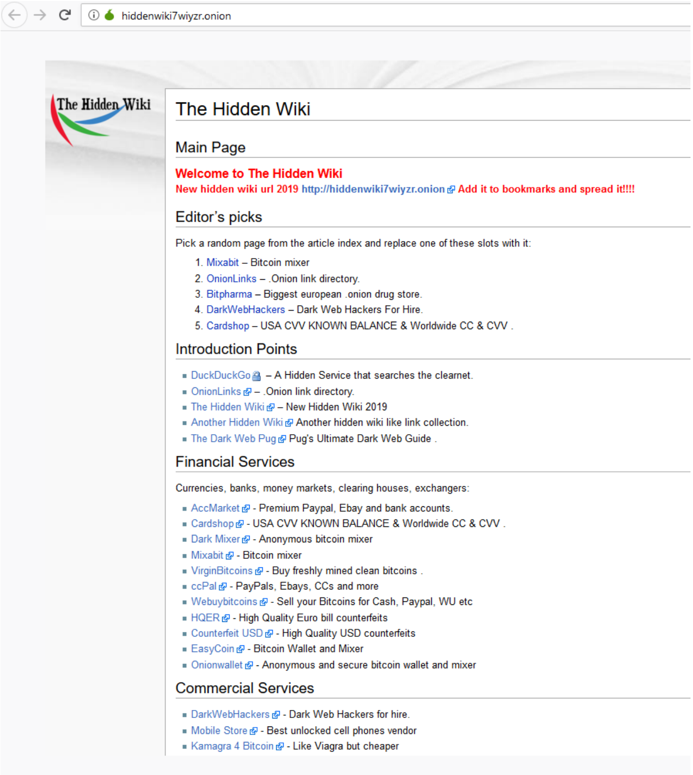
Click "Connect" to connect to Tor.

Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

For assistance, visit support.torproject.org/#connectingtotor

Once you press connect, the browser will do its magic and get you onto the network. You can view any standard website from the browser but remember that your use of Tor may be painfully slow and provide you with multiple `The Connection has timed out` errors depending on your obfuscated connection, some websites may not initially display in English. For example, when typing the address to our good old friends Google in the browser, you may end up on the German version.

As onion links expire and change multiple times, most directories that aren't up-to-date contain multiple onion URLS that lead to nowhere. The best way to find recent and verified onion links is to search for **The Hidden Wiki** which can be found fairly effortlessly by searching for it using a search engine like DuckDuckGo. Whilst nearly every search engine indexes only the Clearnet, you can find the .onion link via a standard website. Several versions of The Hidden Wiki exist with the most popular directory considered 'censored' meaning that whilst plenty of websites selling or supplying illegal information are featured within the directory, sites that encourage, sell or display child porn and murder are not.



hiddenwiki7wiyzr.onion

The Hidden Wiki

The Hidden Wiki

Main Page

Welcome to The Hidden Wiki

New hidden wiki url 2019 http://hiddenwiki7wiyzr.onion Add it to bookmarks and spread it!!!!

Editor's picks

Pick a random page from the article index and replace one of these slots with it:

1. Mixabit – Bitcoin mixer
2. OnionLinks – .Onion link directory.
3. Bitpharma – Biggest european .onion drug store.
4. DarkWebHackers – Dark Web Hackers For Hire.
5. Cardshop – USA CVV KNOWN BALANCE & Worldwide CC & CVV .

Introduction Points

- DuckDuckGo – A Hidden Service that searches the clearnet.
- OnionLinks – .Onion link directory.
- The Hidden Wiki – New Hidden Wiki 2019
- Another Hidden Wiki Another hidden wiki like link collection.
- The Dark Web Pug Pug's Ultimate Dark Web Guide .

Financial Services

Currencies, banks, money markets, clearing houses, exchangers:

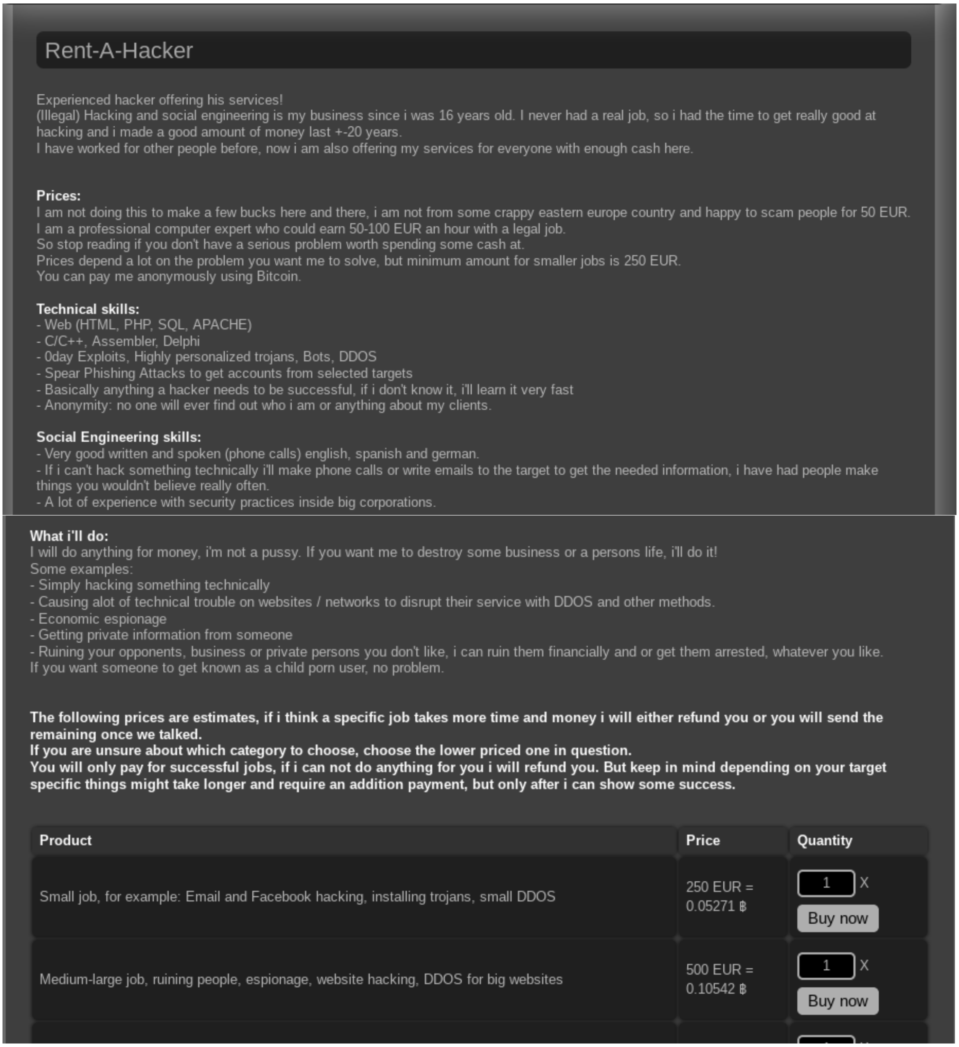
- AccMarket - Premium Paypal, Ebay and bank accounts.
- Cardshop - USA CVV KNOWN BALANCE & Worldwide CC & CVV .
- Dark Mixer - Anonymous bitcoin mixer
- Mixabit - Bitcoin mixer
- VirginBitcoins - Buy freshly mined clean bitcoins .
- ccPal - PayPals, Ebays, CCs and more
- Webuybitcoins - Sell your Bitcoins for Cash, Paypal, WU etc
- HQER - High Quality Euro bill counterfeits
- Counterfeit USD - High Quality USD counterfeits
- EasyCoin - Bitcoin Wallet and Mixer
- Onionwallet - Anonymous and secure bitcoin wallet and mixer

Commercial Services

- DarkWebHackers - Dark Web Hackers for hire.
- Mobile Store - Best unlocked cell phones vendor
- Kamagra 4 Bitcoin - Like Viagra but cheaper

Crypto-currencies like Bitcoin are essentially the only currency accepted on any Dark Web marketplace. Marketplaces come and go – some will genuinely sell you illicit drugs that may or may not arrive in the mail and some will simply steal your money and leave you with no choice but to accept it. Visiting your local police station to report a scammer who took your anonymised money and never delivered the big bag of illicit drugs you ordered is not advisable.

Many of the onion links have reviews that require decent research due to the ambiguity of the services provided. The below screenshot is a website that is listed on one of the Hidden Wiki mirrors which lists what has been verified by multiple users and what has been reported as fake.



Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my business since i was 16 years old. I never had a real job, so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now i am also offering my services for everyone with enough cash here.

Prices:
I am not doing this to make a few bucks here and there, i am not from some crappy eastern europe country and happy to scam people for 50 EUR.
I am a professional computer expert who could earn 50-100 EUR an hour with a legal job.
So stop reading if you don't have a serious problem worth spending some cash at.
Prices depend a lot on the problem you want me to solve, but minimum amount for smaller jobs is 250 EUR.
You can pay me anonymously using Bitcoin.

Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i don't know it, i'll learn it very fast
- Anonymity: no one will ever find out who i am or anything about my clients.

Social Engineering skills:
- Very good written and spoken (phone calls) english, spanish and german.
- If i can't hack something technically i'll make phone calls or write emails to the target to get the needed information, i have had people make things you wouldn't believe really often.
- A lot of experience with security practices inside big corporations.

What i'll do:
I will do anything for money, i'm not a pussy. If you want me to destroy some business or a persons life, i'll do it!
Some examples:
- Simply hacking something technically
- Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
- Economic espionage
- Getting private information from someone
- Ruining your opponents, business or private persons you don't like, i can ruin them financially and or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.

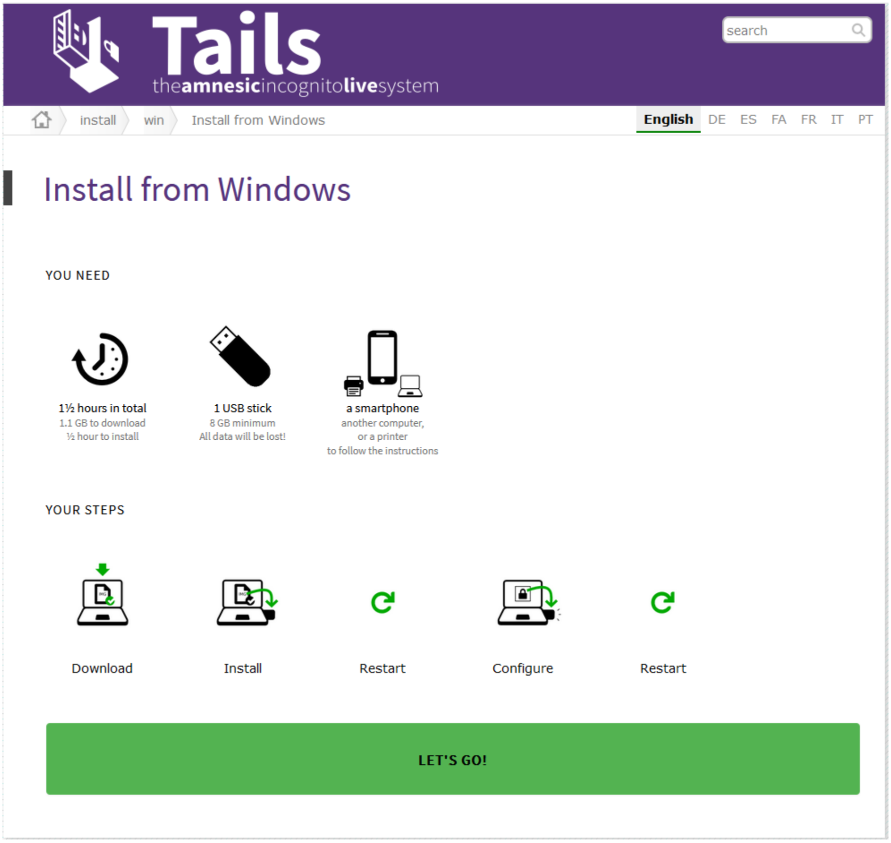
The following prices are estimates, if i think a specific job takes more time and money i will either refund you or you will send the remaining once we talked.
If you are unsure about which category to choose, choose the lower priced one in question.
You will only pay for successful jobs, if i can not do anything for you i will refund you. But keep in mind depending on your target specific things might take longer and require an addition payment, but only after i can show some success.

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.05271 ฿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.10542 ฿	1 X Buy now

Option two – the far safer one – is to set up Tails.
Tails is **T**he **A**mnesic **I**ncognito **L**ive **S**ystem and requires a little more effort but is essential if you plan on staying as private as possible when searching for whatever content it is you are looking for, whether it be frowned upon in your country or something that could land you in jail.

All you need is an internet connection, a USB drive that has at least 8GB of storage space (or DVD burner and blank disc) and a computer.
To download Tails, visit ***https://tails.boum.org*** from your standard computer or mobile device (although you won't be able to install the system via mobile, you can certainly download it through your cellular connection)
The file you download will be a `.img` file that is just over 1GB in size. Most browsers have a Tails Verification extension that will verify the file you downloaded is free from interference. This all occurs within the download page, so don't think too much about that – although it's fast and advisable, it's not required.

The tails website provides an easy-to-follow guide that covers setting everything up from Windows, Mac and Linux operating systems.



Install from Windows

YOU NEED

1½ hours in total
1.1 GB to download
½ hour to install

1 USB stick
8 GB minimum
All data will be lost!

a smartphone
another computer,
or a printer
to follow the instructions

YOUR STEPS

Download

Install

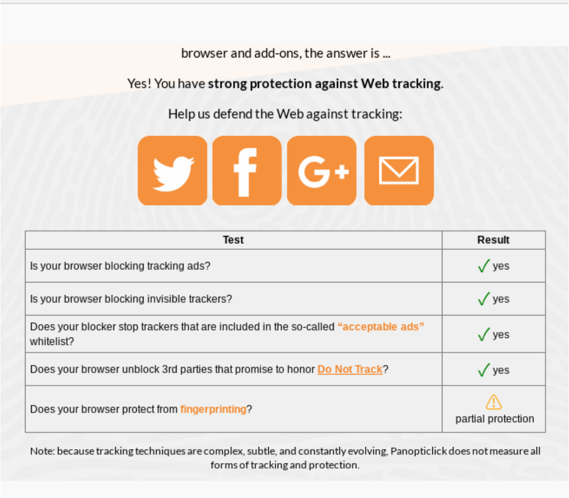
Restart

Configure

Restart

Once downloaded, proceed to the next pages on the Tails website which will provide further details on how you can put that `.img` file onto a USB drive (or disc) and launch the live OS on your computer.

If you have additional concerns about tracking, you can install Tails from within another Tails operating system. The sky is the limit when trying to be elusive as possible. If you're worried about any potential bread trails, you can install Tails from Windows, then use that Tails operating system to install another Windows or Linux operating system and so forth. This may seem excessive, but it is an option. Tails itself has an inbuilt installer that can clone or build another version of Tails should you wish to evade any possibility that the USB drive you installed it on can identify the computer you set up the initial Tails OS on.



browser and add-ons, the answer is ...

Yes! You have **strong protection against Web tracking**.

Help us defend the Web against tracking:

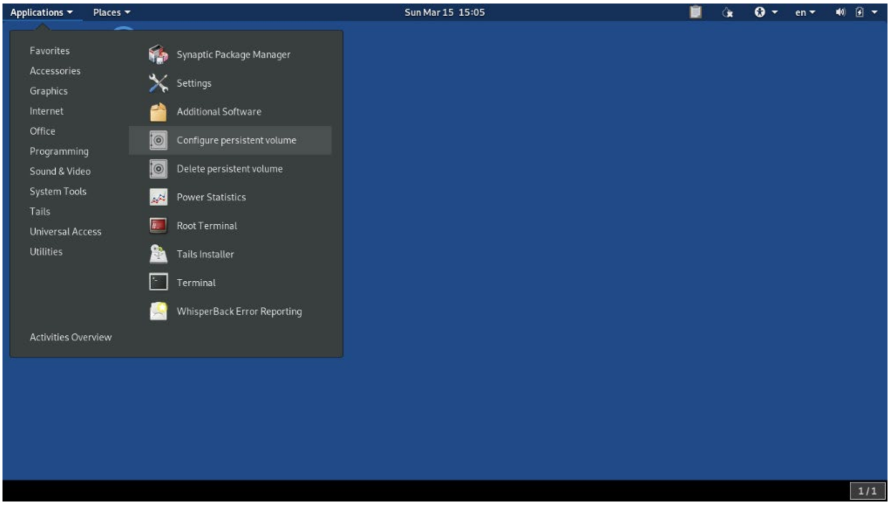
Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your blocker stop trackers that are included in the so-called "acceptable ads" whitelist?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✓ yes
Does your browser protect from fingerprinting?	⚠ partial protection

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

The screenshot above shows that the Tor Browser ranks highly on the EFF Browser Test website suggested in the previous section. The warning of partial protection can be ignored as the browser has successfully given false information.

Another handy feature is a persistent storage volume; an encrypted section of the USB drive you may wish to store information on for access at a later date using a passphrase (a series of words, rather than a single password without letters). Whilst storing legally questionable content from the Dark Web on any USB drive isn't advised regardless of encryption, it's a great way to maintain a secure location of files – even if you're looking to securely store documents and not have the Tails OS ever connect to the internet. Persistent storage can also be used to store details such as network connections, browser bookmarks or secret access keys.

To set this up simply jump onto your Tails OS and select the **Applications** menu and find **Configure persistent volume** under **System Tools** or **Tails**.



You can also delete the persistent storage after you've finished with the drive. If you're concerned about the drive and what it may still contain on it, you can physically destroy the USB by smashing it or removing the storage chips on the circuit board. The internals of a USB drive tend to survive washing machines and many harsh chemicals. You can also transfer files saved from your live Tails drive by inserting another USB drive into the computer or laptop. As Tails is a Linux distribution, the other drive will appear as a standard storage system you can transfer files to and from.

Be sure to read the "Warnings and limitations" page on the Tails website to guarantee that your overall environment is safe and that any flaws within your network or computer hardware can be sorted before using Tails.

Though it's the most popular, Tor is not the only service available.
Alternatives include the Invisible Internet Project (I2P)
FreeNet which has since been discontinued and so may be vulnerable.

SECURE COMMUNICATION

Throughout time there have been many ways of securely communicating without government or police interference. In the age of electronics this has included burner phones, payphones, internet cafes or good old fashion physical methods such as writing a note and shredding it into thousands of tiny pieces which is actually a method Edward Snowden used to disclose information to interviewers in the 2014 documentary *CITIZENFOUR*.

Whilst whistleblowers can use services such as the Freedom of the Press Foundation's submission system SecureDrop[13] and there are plenty of services and applications – each with their own merits and shortcomings – to communicate with people online.

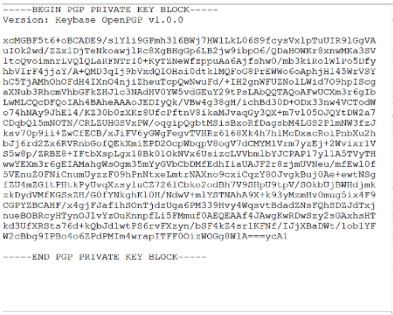
PGP – Pretty Good Privacy – is almost universally considered to be the most reliable and secure way to send a message to another without the worry of snooping.

Several free and premium software applications for encrypting, decrypting and storing keys (often referred to as keyrings) exist. Whilst often referred to as PGP keys due to the exact same standards being used the free, interchangeable, implementation is in-fact known as GnuPG (or GPG)

The creator of PGP, Phil Zimmermann, wrote the program in 1991 to help activists and those seeking to maintain secrecy online safeguard their communications. The invention of such a tool was a violation of U.S. law and saw Zimmerman formally investigated by the United States government when use of the tool began to disperse outside of the States.

[13] https://securedrop.org/directory/

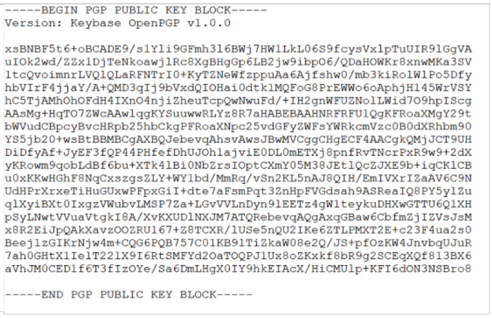
PGP keys are given in pairs: A private key for you to hold onto and never share, and a public key to give out to anyone wishing to securely contact you. The below example is a basic PGP key pair. Depending on the encryption setting chosen, the keys (often `.asc` or `.pgp` files – though simply text files containing the key characters regardless of the file extension) some keys may feature as many as 4000 characters.



```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Keybase OpenPGP v1.0.0

xcMGBF5t6+oBCADE9/s1Yli9GFmh3l6BWj7HW1LkL06S9fcysVxlpTuUIR9lGgVA
uIOk2wd/ZZx1DjTeNkoawjlRc8XgBHgGp6LB2jw9ibpO6/QDaHOWKr8xnwMKa3SV
ltcQvoimnrLVQlQLaRFNTrI0+KyTZNeWfzppuAa6Ajfshw0/mb3kiRolWlPo5Dfy
hbVIrF4jjaY/A+QMD3qIj9bVxdQIOHai0dtklMQFoG8PrEWWo6oAphjH145WrVSY
hC5TjAMhOhOFdH4IXnO4njiZheuTcpQwNwuFd/+IH2gnWFUZNolLWid7O9hpIScg
aXNub3RhcmVhbGFkZHJlc3NAdHV0YW5vdGEuY29tPsLAbQQTAQoAFwUCXm3r6gIb
LwMLCQcDFQoIAh4BAheAAAoJEDIyQk/VBw4g38gH/ichBd30D+ODx33nw4VCTodW
o74hNAy9JhEl4/KZ30b0zXKz8UfcPftnV8ikaMJvaqGy3QX+m7vl05OJQYtDW2a7
CDqbQl5mNOTN/CRLZUHGSVxPW/oqgipQgbtMSisBxoRfDagsbM4LGS2PlmNW3fzJ
kav70p9ii+ZwCfECB/xJiFV6yGWgFegvTVHRz6l68Xk4h7hlMcDxacRoiPnbXu2h
bJj6rd2Zx6RVRnbGofQEkXmiEPD2OcpWbqpV8ogV7dCMYM1Vrm7yzEj+2Wvixr1V
S5w8p/ZRBE8+IFtbXspLgx18Bk01OkNVx6UsizcLVVbmlbYJCPAP17yl1A5TVyTH
wwYEXm3r6gEIAMahgWsOgm35mYyGVbCbDMfEdhIiaUAJF2r8zjmUVNeu/mfEwl0f
5VEnuZ0FNiCnumUyzzF09hPnNtxeLmtrNAXno9cxiCqzY8OJvgkBuj0Ae+ewtNSg
fZU4mZGltPHtkPyUvqXzsyluCZ726lCbke2odBh7V9SHpU9tpV/SOkbUjBWHdjmk
zkDydVMfKGSsZH/G0fYNkghKl0H/NdwV+mlYSTNAhA9X+k93yMzmHv0mug5ix4F9
CGPYZBCAHF/x4gjFJafihSOnTjdzUga6PM339Hvy4WqsvtBdadZNsFQhSDZJdTxj
nueBOBRcyHTynOJlvYzOuKnnpfLi5FMmuf0AEQEAAf4JAwgKwRDwSzy2sGAxhsHT
kd3UfXRSts76d+kQbJdlwtPS6rvFXzyn/bSF4kZ4srlKFNf/IJjXBaDWt/1oblYF
W2cBbq9IPBo4o6ZPdPMIm4wrapITFF0OizWOGg8WlA===ycA1

-----END PGP PRIVATE KEY BLOCK-----
```



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Keybase OpenPGP v1.0.0

xsBNBF5t6+oBCADE9/s1Yli9GFmh3l6BWj7HW1LkL06S9fcysVxlpTuUIR9lGgVA
uIOk2wd/ZZx1DjTeNkoawjlRc8XgBHgGp6LB2jw9ibpO6/QDaHOWKr8xnwMKa3SV
ltcQvoimnrLVQlQLaRFNTrI0+KyTZNeWfzppuAa6Ajfshw0/mb3kiRolWlPo5Dfy
hbVIrF4jjaY/A+QMD3qIj9bVxdQIOHai0dtklMQFoG8PrEWWo6oAphjH145WrVSY
hC5TjAMhOhOFdH4IXnO4njiZheuTcpQwNwuFd/+IH2gnWFUZNolLWid7O9hpIScg
AAsMg+HqTO7ZWcAAwlqgKYSuuwwRLYz8R7aHABEBAAHNRFRFU1QgKFRoaXMgY29t
bWVudCBpcyBvcHRpb25hbCkgPFRoaXNpc25vdGFyZWFsYWRkcmVzc0B0dXRhbm90
YS5jb20+wsBtBBMBCgAXBQJebevqAhsvAwsJBwMVCggCHgECF4AACgkQMjJCT9UH
DiDfyAf+JyEF3fQP44PHfefDhUJOhlajviE0DL0mETXj8pnfRvTNcrPxR9w9+2dX
yKRowm9qobLdBf6bu+XTk4lBi0NbZrsIOptCXmY05M38JEtlQcZJXE9b+iqCKlCB
u0xKKwHGhF8NqCxszgsZLY+WY1bd/MmRq/vSn2KL5nAJ8QIH/EmIVXrIZaAV6C9N
UdHPrXrxeTiHuGUxwPFpxGiI+dte7aFsmPqt3ZnHpFVGdsah9ASReaIQ8PY5ylZu
qlXyiBXt0IxgzVWubvLMSP7Za+LGvVVLnDyn9lEETz4gW1teykuDHXwGTTU6Q1XH
pSyLNwtVVuaVtgkI8A/XvKXUDlNXJM7ATQRebevqAQgAxqGBaw6CbfmZjIZVsJsM
x8R2EiJpQAkXavzOOZRU167+Z8TCXR/lUSe5nQU2IKe6ZTLPMXT2E+c23F4ua2s0
BeejlzGIKrNjw4m+CQG6PQB757C01KB9lTiZkaW08e2Q/JS+pfOzKW4JnvbqUJuR
7ah0GHtX1IelT22lX9I6RtSMFYd2OaTOQPJ1Ux8oZKxkf8bR9g2SCEqXQf813BX6
aVhJM0CED1f6T3fIzOYe/Sa6DmLHgX0IY9hkEIAcX/HiCMUlp+KFI6dON3NSBro8

-----END PGP PUBLIC KEY BLOCK-----
```

The following pile of random characters is an encrypted message that has been encrypted using the Public key block above:

```
-----BEGIN PGP MESSAGE-----
Version: OpenPGP v2.0.8
wcBMA8etPZQwEJoaAQgAnnAi5Nzf5pZ/n+aQXQDwV0kLPDI3bOXo6JSNRtFM7xtT
oBSlCdFp0X+hEOsfR/GvmQkQqi1jkDqTWPXdqQhk3ys3vNFY5W70xfuFDR71vkT0
36iI0laWTEC2r9Al1SVSarTiYD/M4BTp5vl8dFH36SuaqPycOOht5CqjnH7hyBMl
0gqw3ny6d9RdSD3cD6VbaInJq53cHojz773+4SWZlt0QqGIKrcd5dn+nFutpyZ/3
KWzkBrRYW5Lloy12WZ4TgedZkeLz76rAiOSRCVtXJqL7E//edCdZBJhXwNU5jML5
Q9YIOg1ejpwvTmzD74xX21E7JGgtE5HFPLUqRzArJtJ+AevC6UeJn2U++hvHYeCS
zl6VivYWYR2O3gGOzjTJkWkBjSCEezm/Qv60DhO9jpFAgzJkPoOzkByKaLs/u9eU
bjjbyqUecSGRRN0UXSPJFYQ5L7CcJpaDf3ZSBqdcaI+uk4r09SkljnX3BHJwm5EC
I4kfRl3K3T0ZbBaKQRjr
=gBEn
-----END PGP MESSAGE-----
```

When received by the party holding the private PGP key and passphrase, it can be decrypted by pasting the mass of characters into a software or browser-based PGP tool. The decrypted message reads:

```
This message is going to be encrypted and then
decrypted by as an example for a book.
Sorry it wasn’t more interesting.
```

Whilst the key file can be uploaded to the internet as a text file or one of the extensions provided by the key generating application, a smaller series of code called a fingerprint can be used as a more-convenient method of displaying it on a business card or online profile.
For example, the public key shown above has the PGP fingerprint:

```
7B31 C9A7 9020 368E B202 EE3C 3232 424F D507 0E20
```

Several applications and extensions exist for mail clients like Outlook, Thunderbird and Apple Mail. Windows has multiple free software applications such as **Gpg4win**. When generating a key pair with most software you also have the ability to choose the security level of the key (the higher the security, the larger the key files) and you can even set an expiry date so that a key will be unusable after a certain period of time.

PASSWORDS MATTER —BUT THERE ARE BETTER OPTIONS

Whilst I won't sit here and explain how passwords such as `123456` and `password` are terrible ideas unless you want all of your data and devices accessed by people with questionable intention; the password itself isn't truly secure, even if it is made up of random words, numbers and special characters. Security directory *SecLists*[14] contains a somewhat alarming list of usernames and passwords that have been traced by multiple tools attempting to decipher them and gain access. As found in the websites suggested previously, breaches show just under 40% on average of passwords retrieved by hacking tools are unique.

You've no doubt grown sick of being told *"don't use the same passwords and security question and answers"* and *"don't use names of family, friends and animals"* and that is absolutely understandable. If a password like `auntierose!1942` is easy to remember and secure enough, why would you opt for dozens of impossible to recall passwords across multiple different accounts like: `r%Zh+D532AhENq%`

[14] https://github.com/danielmiessler/SecLists

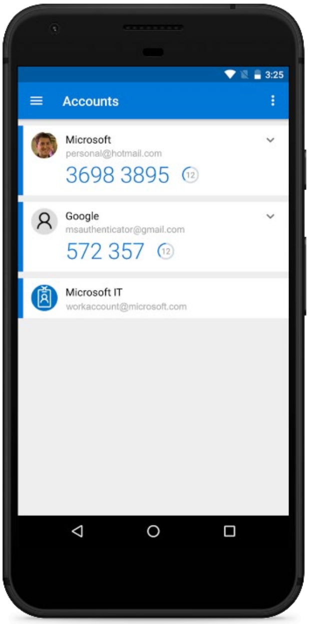
Fortunately, there are much better options like password managers such as LastPass or the open-source KeePass, RoboForm and my Bitwarden (which I recommend) and you'd likely be best avoiding having passwords stored in the cloud despite the inconvenience.

Note: KeePass has two derivatives known as *KeepassX* and *KeePassXC*, the latter of which is endorsed by the EFF.

Whilst password managers are great for generating and then storing a random almost unguessable password, there are much better authentication standards – most of which can coexist with passwords and password managers.
The FIDO Alliance, which stands for **F**ast **ID**entity **O**nline, is an open industry association promoting stronger authentication across all platforms. Technologies like biometrics, voice and facial recognition and fingerprint and eye scanners may not be truly flawless or even private but they do give a user a much easier and safer way to protect their information.

Authenticator applications provided by multiple corporate and community-based developers are easily available and carry on the methods ***Multi-Factor authentication*** and **Two-factor authentication** (2FA)
An example of 2FA in action is as follows:
You log into your computer from an unfamiliar device > You receive a page informing you that you need to verify your identity > You receive a text message on a connected phone, or an email to the connected address > You type in the number or click the link and voila: your device is verified and you can proceed

Other methods include ***One-Time passwords*** known as ***OTP*** (similar to the 2FA method) that send a password phrase or number to your connected phone number, application or



Microsoft
personal@hotmail.com
3698 3895

Google
msauthenticator@gmail.com
572 357

Microsoft IT
workaccount@microsoft.com

Microsoft's Authenticator application using TOTP

account which expires as soon as you use it. A ***Time-based One-Time Password*** known as **TOTP** is an extension of the method but involves the password expiring within a certain period of time (usually 30 seconds)

Some Authenticator applications incorporate the above methods, but with a fingerprint, face, PIN or generated code. In some cases, you'll be given a trio of different double-digit numbers on your phone with the computer application telling you which one to tap.

Software authenticators are great and convenient, but physical options take the idea of having a house key for your devices.

FIDO standardises the use of physical hardware for authentication. Options like USB security keys and even mobile applications are the sure-fire way to increase your password security. You can even set up your smartphone to act as a physical security device by unlocking your device via NFC (Near Field Communication) or Bluetooth.
USB keys are an interesting solution: products like the YubiKey by Yubico[15] look like standard USB drives and physical keys, but give users the option to choose between a tiny USB drive that stays plugged in or a key that can be touched to authenticate. There are also versions that support NFC and also can be plugged into USB-C and Lightning ports like found on smartphones and supported devices. Other

[15] https://www.yubico.com/

products include *SoloKeys*, *OnlyKey* and *Nitrokey* to name a few. Although popular physical keys can be somewhat expensive depending on their features, it's important to consider cheaper, lesser-known brands may have security vulnerabilities or even physical weaknesses. A good USB key manufacturer should also give you the ability to verify the device and know the locations and stringent security and quality controls involved.

YubiKey 5 NFC which can be used with Windows, Android and iOS and is incredibly hard to destroy.

DEVICE PRIVACY

This could be an entire book in itself, so let's address the main issues that can risk the security of your device.

MOBILE:
Portable devices have become increasingly powerful, but with great power comes great battery drain. Many airports, shopping centres and restaurants offer charging kiosks or charge stations intended for those requiring a boost. It's theoretically possible that connecting to one of these USB ports puts you at the risk of data transfer. This is referred to as ***juice jacking.***
Criminals can implement a system that takes the data from your phone and sends it wirelessly – or stores it on a concealed drive that can be collected at a later date. Data theft is not the only way. Connecting to a compromised USB port can lead to malware being installed onto your device.
There are also cases where criminals have left cables plugged in at charging stations that contain a concealed way of storing any data while you're charging; possibly gluing the USB cable into the kiosk or station preventing you from taking the cable with you. In Theory, this could also be possible by false companies handing out infected USB cables as promotional merchandise. The cables could transfer data via your computer if ever plugged in or transfer malware to both your phone and computer for wireless theft.

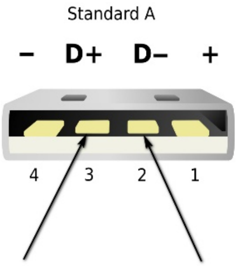
Here are a few suggestions to prevent this:
1 – Take a portable power bank with you. This way you can charge the power bank when it is low at a charge station without risking any data transfer. Your device can then charge from the power bank.

2 – Carry an adapter with you. Many locations with charging stations also allow users to charge their laptops or non-USB devices through a power outlet.

3 – If you really need to charge your device and don’t have any of these facilities available, shut down your device before connecting it via USB.

4 – Use a cable that is two-conductor. This means it only has the ability to charge. You can either cut the wires inside an all-purpose cable or purchase one that can only be used for charging. An easy way to test if your cable is two-conductor is to connect it to a computer and see if the computer recognises the device. If it does; you have a power + data-transfer cable.

5 – Use a “USB Condom” – as the name alludes, these are protective adapters that disable the data transfer pins on the USB cable. The cable will charge your device, but it won’t be able to transmit data. Commercial versions such as Portapow, Kryptall and Syncstop exist and many similar adapters are available known as *‘data blockers’* or *‘juice jack defenders.’* These adapters are fancy looking and act as a go-between, but the premise is fairly simple. If you look inside a USB cable you will see four gold contacts. The outer contacts are for power, whilst the inner contacts are for data transfer. With some careful precision, you can use a piece of tape to block these contacts. Be careful not to block the outer ones as shown:

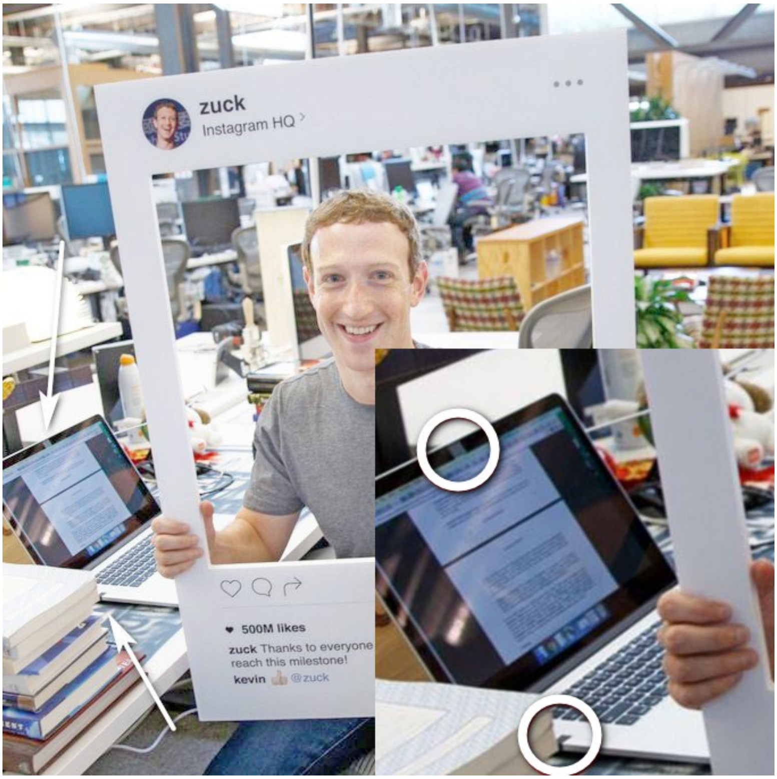


There are limitations to USB condoms and data pin blocking. Quick charge will not work or charging speeds will be slower.

COVER YOUR CAMERA

As suggested previously, if your device has an internal camera. Cover it when not in use.
If your camera is external – disconnect it. If disconnecting it is inconvenient due to frequent use, then camera covers exist – usually purchasable in a pack of multiple numbers. There are also sticker-type alternatives for embedded cameras on your laptop, TV or phone. Covers are a cheap and friendly option but won't block microphone audio.

So why bother covering your camera?
Well as explored in the book it's a great spy tool – even if you have nothing to hide. Simply being hacked gives people the 'eyes' into your life and can find a way to exploit you – even if it is just footage of you picking your nose!



Another reason? Because Facebook's Mark Zuckerberg does it. That's enough to scare anyone. In 2016 Zuckerberg revealed he was delighted to announce that Instagram had reached 500 million users. In the photo posted on Facebook celebrating this achievement, it appears that the Zuck himself blocks his microphone (or audio jack) and camera with tape!

FILE ENCRYPTION

There's not much point in following all the security advice featured within the book, if your files are available for all to see. Should you have files or a USB drive (or a whole internal drive) you want to lock down you have multiple ways of doing this using inbuilt encryption offered by most operating systems or third-party software which provides that little extra trust.

TrueCrypt has been regarded as the safest and most-trusted software despite its lack of development. TrueCrypt was used by Glen Greenwald to encrypt Edward Snowden's leaked materials between Brazil and Berlin. In 2014 the website featured the ominous message "WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues" following a guide on using Windows' built-in features - a rather dubious suggestion given the concern brought about with the NSA leaks.
The release of version 7.2 has the warning "You should download TrueCrypt only if you are migrating data encrypted by TrueCrypt."

An independent crowdfunded audit into TrueCrypt 7.1a by American software engineer and security researcher Steve Gibson's Gibson Research Corporation confirms the safety and security of using TrueCrypt 7.1a and hosts the audited installation packages for the available platforms. As the software was developed by a small volunteer team who never revealed their identities, when the project was abandoned nobody was able to ask to take-over. Gibson Research, however, confirms that one of the TrueCrypt developers contact the team stating their approval of the audit and the software was simply dropped due to lack of interest.

A modern ‘fork is VeraCrypt which is also free. VeraCrypt exists for Windows, Mac OS X and Linux users. VeraCrypt is based on the original TrueCrypt 7.1a software with additional enhancements but is technically unofficial and unendorsed.

LINKS:

https://blog.cryptographyengineering.com/2015/04/02/truecrypt-report/
https://www.grc.com/misc/truecrypt/truecrypt.htm
https://opencryptoaudit.org/
https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf
https://github.com/veracrypt/VeraCrypt

DATA AND DEVICE DESTRUCTION

Maybe you're thinking a hammer to your laptop, phone or USB drive is the best way to go? Or maybe you feel you should really protect yourself by destroying the device properly.

You don't have to go as far as grinding circuit boards with rotary tools like *The Guardian* did under GCHQ pressure, but there are some very sensible and easy ways to destroy data and devices to ensure any trace of information can never be recovered.

When you select a hard drive to format in your OS you are often given the ability to perform a quick format. Quick formatting a device allows the data stored on it to be recovered easily, even with free tools aimed at restoring lost data. When you delete a disk file, you don't really *remove* it, you just clean it out so that when new files are created, they see the free space. A full format takes a bit longer – and can take days depending on the speed of your hard drive and computer – but will securely remove the data. However, it's still possible that the data is not gone for good. Forensic data experts will find a way should they need to retrieve the data for whatever reason. If you are worried about this, then you should consider destroying the drive as detailed later. If you want to keep the drive and simply format it or delete a few files you have a couple of options: delete the files with software *shredders* or *secure delete* programs of which many open-source and trustworthy applications exist.

To completely clean a drive, you will need to low-level format it – in modern terms this is referred to as performing a zero-fill.

A zero-fill literally writes zeros to a hard drive, replacing all data and preventing recovery. As with all issue's security-wise; you should exercise precaution as the data may be recoverable using hardware-based recovery. Zero-filling *should* make it impossible for software to recover the files. Disk drive manufacturers like Seagate, Western Digital and Hitachi all offer free applications dedicated to doing this job within the Operating System. If you trust your OS, then Windows, Mac and Linux all offer the ability to 'sanitise' your drive. For example, Windows users can achieve this through the command line.

Another option is zero-fill outside of the operating system. This can be done using many of the free utilities available by setting up a live USB or Disc and booting from it.

Note that zero-fill methods are intended for magnetic disk storage only and not Solid media such as USB or Flash Memory.

Many operating systems use what is known as a swap file (or a page file). Swap files are temporary memory storage files that allow your computer to continue operating when under heavy load. Image and video thumbnails, text files and fragments of documents can exist in a swap file and when recovered, can give away any illegal or questionable activity performed on the computer.

Physically destroying a storage device is essentially your only option if you truly want to destroy the data, want to go that extra step on-top of zero-filling or the drive has failed and cannot be used with a computer.

For hard disks and mobile devices, you often require obscure tools such as ***Torx*** screwdrivers. These are considered 'secure screws' and come in many obscure shapes that are intended to make the disk or device that little bit more tamper-resistant. Torx screws and various types of 'star' screws are also often easy to locate, but you may need to remove some labels to see the extras.

If it’s a device – rip out as much as you want and do what you want with the pieces, hammers and angle grinders are great. If you’re really concerned, you can dispose of different pieces in different locations. Most devices are not destroyed by water. USB drives and memory cards can be submerged in all sorts of fluids for extensive periods of time and still work. Submerging the disk or flash storage may corrupt the data, but with some replacement circuit boards and motors; the data may still be recovered. A complete download from the Flight Data Recorder – or black box – was successfully completed after the wreckage of *Air France Flight 447* was discovered on the ocean floor in 2011, almost 2 years after the plane went down.

If it’s a disk drive, then you need to make a little more effort. Remove the ‘lid’ of the drive and smash the bright silver platters (disks) inside or scratch them excessively. You can use a blow torch, fireplace, hammer or even a gun. Exercise precaution. Follow sensible safety procedures.

Rather than physically destroying the drive with the excess guide above, you can also encrypt the hard drive with some sort of extreme encryption with an essentially unhackable password and then even opt to drive over it or smash it up a little. If you’re really looking for peace of mind, you can encrypt the drive then go all out and spread the disk’s components through various parts of the city or world. If it could mean your freedom, then go with whatever helps you sleep at night.

Many companies that offer secure document shredding, contraband destruction or even recalled products and counterfeit clothing also offer destruction of computer devices including HDD’s and SSD’s.

This approach is preferred by small businesses, mega corporations and government agencies, especially in countries where privacy laws mandate the secure destruction of staff data. Some companies offer this as an on-site service. One of the methods used for mechanical drives is degaussing: a process in which the HDD is exposed to 20,000 Gauss of raw magnetism. This destroys all data and makes the drive absolutely unusable. If converting your device into fine shrapnel right in front of your very eyes isn’t secure, then this method is not for you.

VIRTUALLY DISAPPEAR FROM THE CLOUD

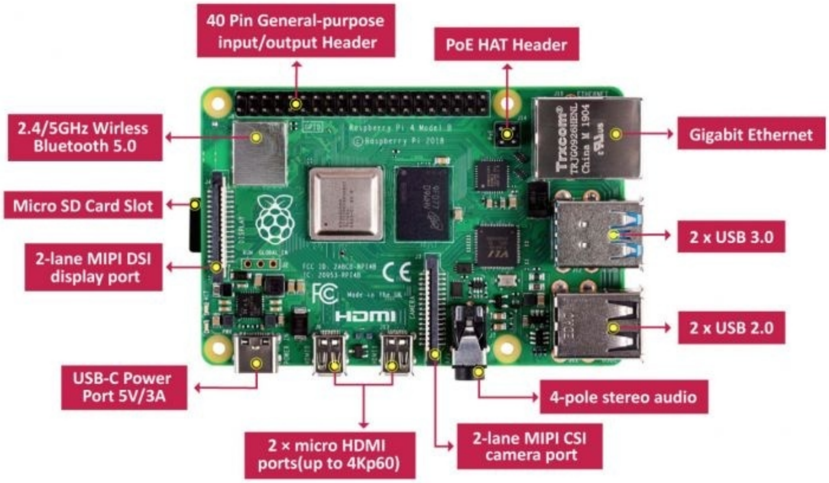
History shows that surveillance takes place even if you've got nothing to hide. With systems out there to target cloud storage providers like Microsoft OneDrive, Google Drive and Dropbox, you may consider setting up your own cloud service. This way you have storage, documents and other applications that can entirely replace your dependency on the major providers.

One of the most popular options is Nextcloud which is an open-source solution that has multiple mobile applications implemented. It acts like your everyday cloud storage provider with installable applications, except you choose the storage options and location. It's your own home cloud that is accessible anywhere providing the box is connected to the internet. You don't need to dedicate a large data server or even a desktop computer to set up Nextcloud.
There are several options including the use of the Raspberry Pi which is easy to conceal or keep out of the way. Western Digital no longer produces the *Nextcloud Box*, which you may be able to purchase pre-owned, but there are other commercial hardware companies offering prebuilt configurations[16]

It's possible to build several of the tiny computers and have yourself a mini data centre with full Pi kits costing less than $100USD.

[16] https://nextcloud.com/devices/

If you use the Raspberry Pi, pre-built images and configuration information is readily available to make the process a breeze[17].


40 Pin General-purpose input/output Header
PoE HAT Header
2.4/5GHz Wirless Bluetooth 5.0
Gigabit Ethernet
Micro SD Card Slot
2 x USB 3.0
2-lane MIPI DSI display port
2 x USB 2.0
USB-C Power Port 5V/3A
4-pole stereo audio
2 × micro HDMI ports(up to 4Kp60)
2-lane MIPI CSI camera port

Raspberry Pi 4 as shown without optional housing accessories – Official case shown below. (images: Raspberry Pi Foundation, UK)

[17] https://ownyourbits.com/nextcloudpi/

FINAL THOUGHTS:

As established in *Under Constant Supervision*, intelligence gathering is now such a high priority to the NSA that it has gone from spying on the United States to spying on the entire world – even their allies.

NSA agents can penetrate a computer for whatever reason they, but they favour non-updated hardware like routers. So first, make sure you change your router password at least once a month. Set yourself a reminder or do it routinely (such as the first day of each month)

Why Tor?
Tor is costly when the NSA wants to track users. It rarely yields the results they hope for. When the NSA requests budget increases from Congress, they are asked how it will benefit and what the result of spending will lead to – and in the case of Tor – it often doesn't lead to much and therefore is a wastage.

What about keeping my data truly hidden?
Have you got data you don't want seen by anyone else? Then buy a laptop and make encrypted storage from it. You can disconnect the internet physically and remove any cameras or microphones from the laptop should you wish to gain better security. Ensure you back up on USB, SD cards or even optical media like DVD or Blu-Ray and ensure the files are encrypted. The only way to truly protect yourself is to act a little paranoid and think as if the police are going to come through the door at any minute and take any computers, phones or portable storage devices they can find. If you are truly concerned about what you are storing on these devices, then go the extra mile and don't become complacent.