# Please, for the Love of God, Make Sure You Delete Things Properly

gizmodo.com/please-for-the-love-of-god-make-sure-you-delete-thing-1832922438

Garbage

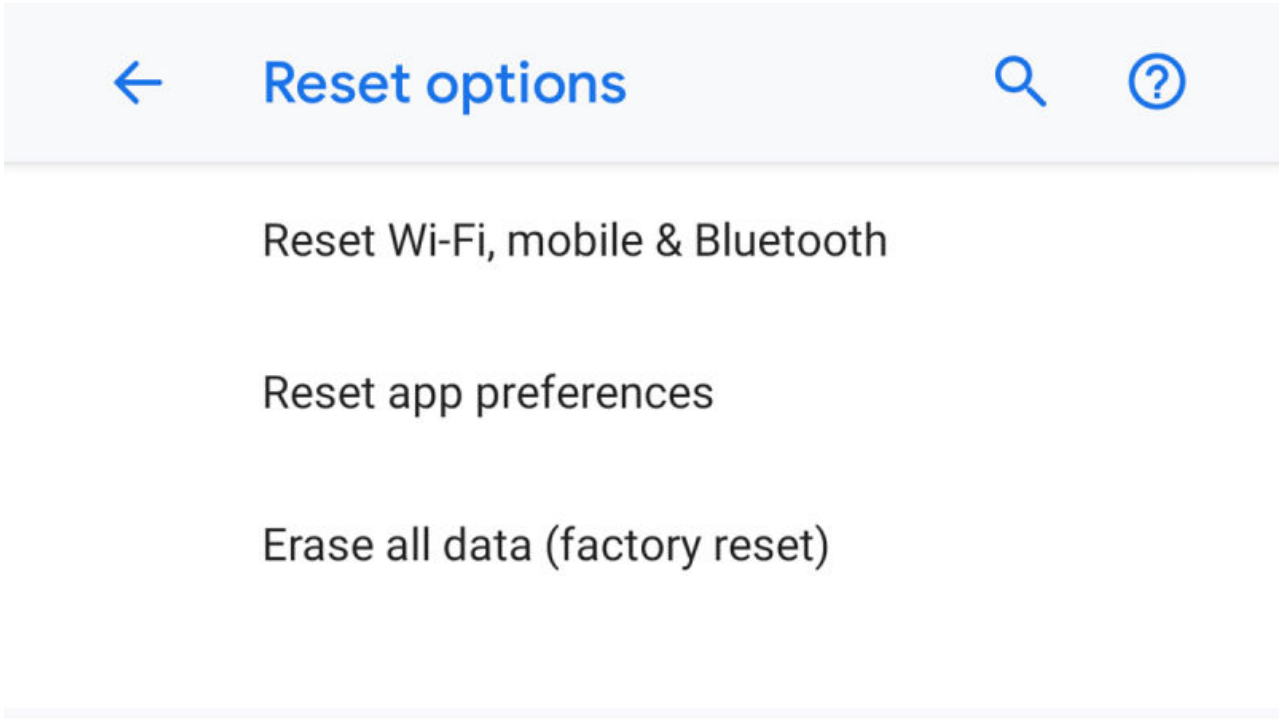

Photo: Fredy Jacob (Unsplash)

GarbageThis week, we are writing about waste and trash, examining the junk that dominates our lives, and digging through garbage for treasure. Your personal data—be it financial spreadsheets or web searches—is not something you want to be leaving behind for other people to find, and totally wiping your activity off devices or the web takes a few more steps than you might have realized. Don't worry though, as we're going to walk you through the process.

## Your smartphone or tablet

So you're selling your phone or tablet, or giving it away to a niece or nephew, or donating it to a museum... whatever the scenario, if it's leaving your possession you want to be absolutely sure everything is gone from it. Having the next owner log into your Twitter

account and flick through your photos is not something you want to happen.

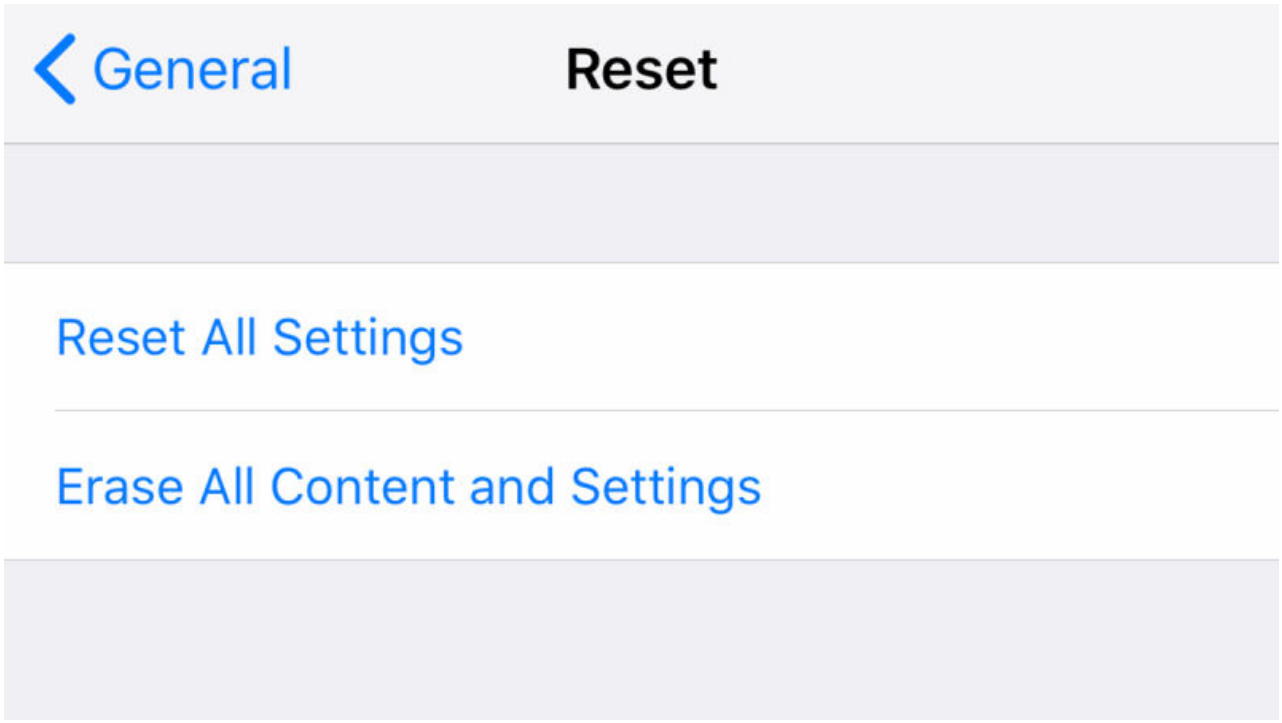



Screenshot: Gizmodo

The good news is it's relatively easy to securely wipe your phone, as long as data on it has been encrypted: This has been standard practice on Android devices since Marshmallow version 6.0 in 2015, and on iOS devices for even longer. As long as you have a PIN, face, or fingerprint to unlock your device, the data is protected.

That encryption means when you factory reset your phone or tablet, it's virtually impossible for anyone to recover the data, even if they pried the storage modules out of your mobile device and tried to read them in another machine. You can double-check your Android device uses encryption by tapping **Security** then **Advanced** in Settings.

To perform a factory reset on Android—after making sure you've taken off and backed up everything you need to, of course—go to Settings then tap **System**, **Advanced**, **Reset options**, and **Erase all data (factory reset)**. Tap through the confirmation prompts to confirm that's what you really want to do, and you're good to go.

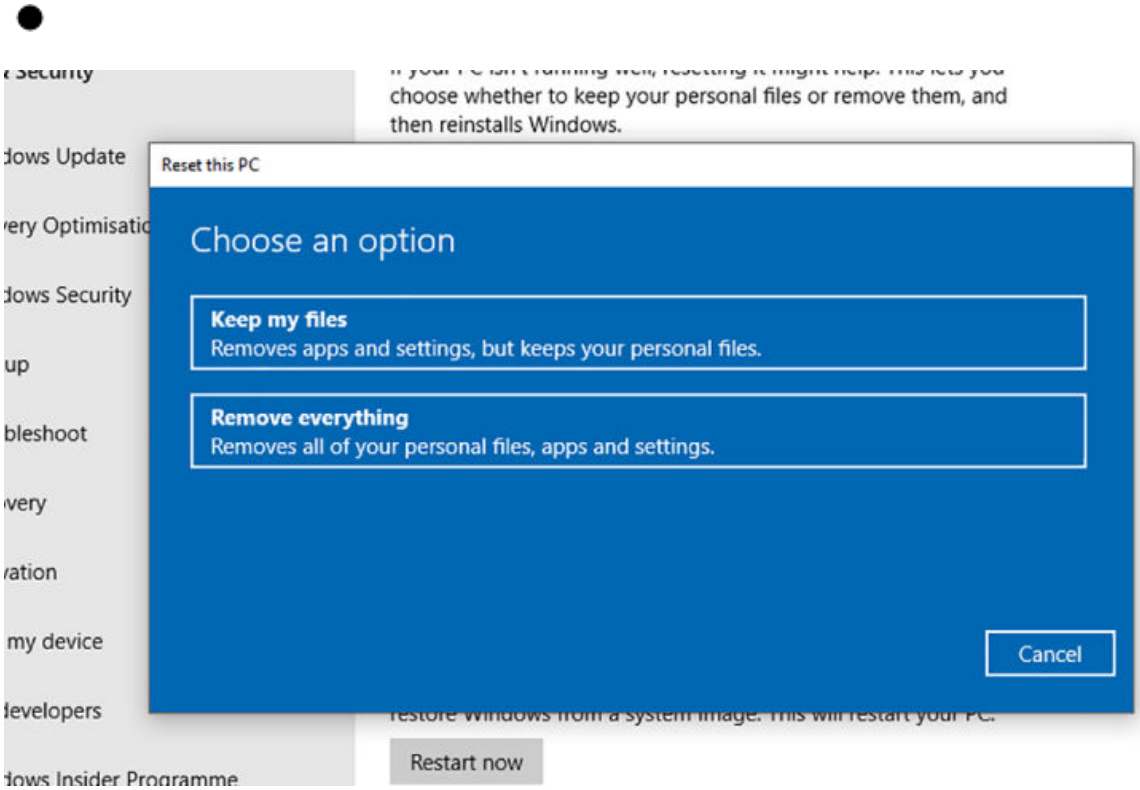



Screenshot: Gizmodo

For those of you using iOS, open up Settings, then choose **General**, **Reset**, and **Erase All Content and Settings** to leave yourself with a factory-fresh phone purged of all your data. Again, don't start the reset process until you're sure you've got your photos, music, and everything else you need safely stored somewhere else.

## Your computer

The same idea applies to your laptop as on your phone, and fortunately modern day Windows and macOS machines are much better at secure wipes than they were once upon a time. Windows 10 doesn't encrypt disks by default (VeraCrypt is good if you're in the market for this extra protection), but it can securely erase files during a reset.

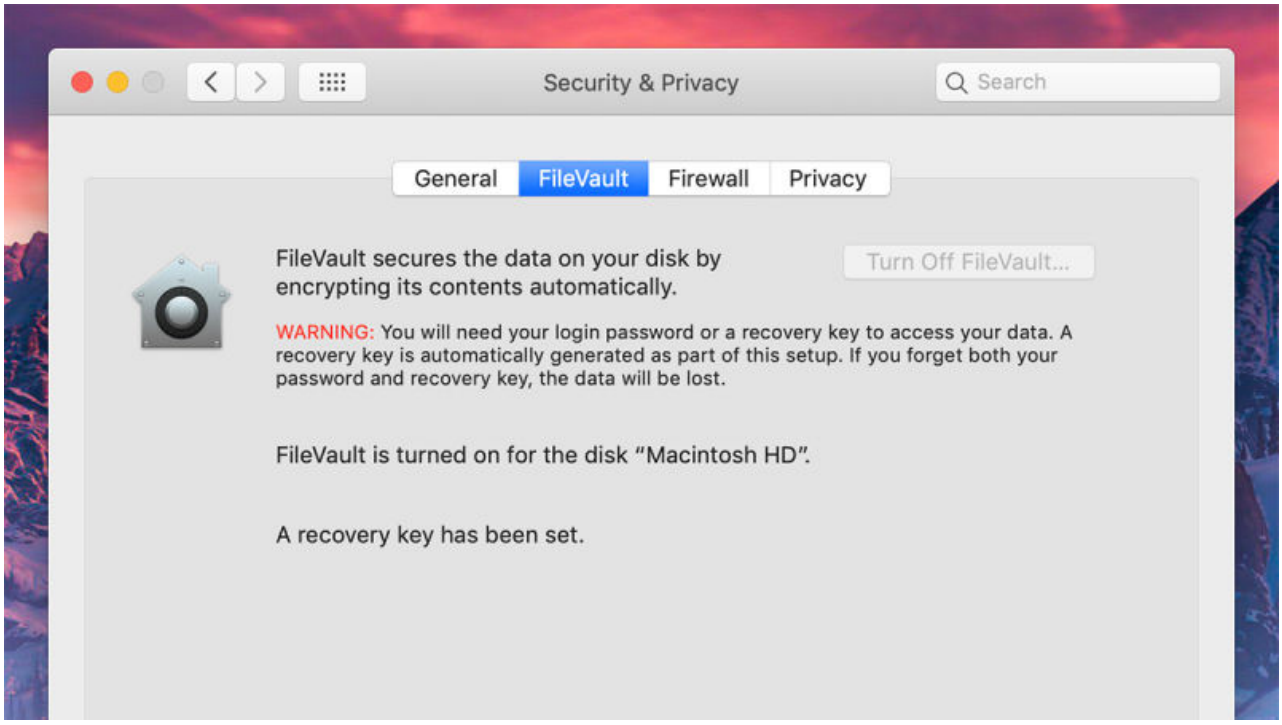



Screenshot: Gizmodo

That means it puts files beyond the reach of data recovery programs and third parties who might want to pick data off your hard drive after you're done with it. With your important data backed up, open Windows Settings, then choose **Update & Security** and switch to the **Recovery** tab. Click **Get started** under **Reset this PC**, choose **Remove everything**, and then make sure you pick **Remove files and clean the drive** on the next dialog.

Wiping and resetting macOS computers is also straightforward: They've been encrypted by default since OS X Yosemite 10.10 (2014) onwards via a tool called FileVault. To make sure it's up and running, open the **Apple** menu, click **System Preferences**, then choose **Security & Privacy** and **FileVault**. If it's not been enabled for whatever reason, you can do that here.

Encrypted data is virtually impossible to recover, so you know a full reset means a full reset—ensure all your personal data and important files are safely copied somewhere else before you start. Open the **Apple** menu, choose **Restart**, then hold down **Cmd+R** as your machine starts up again.

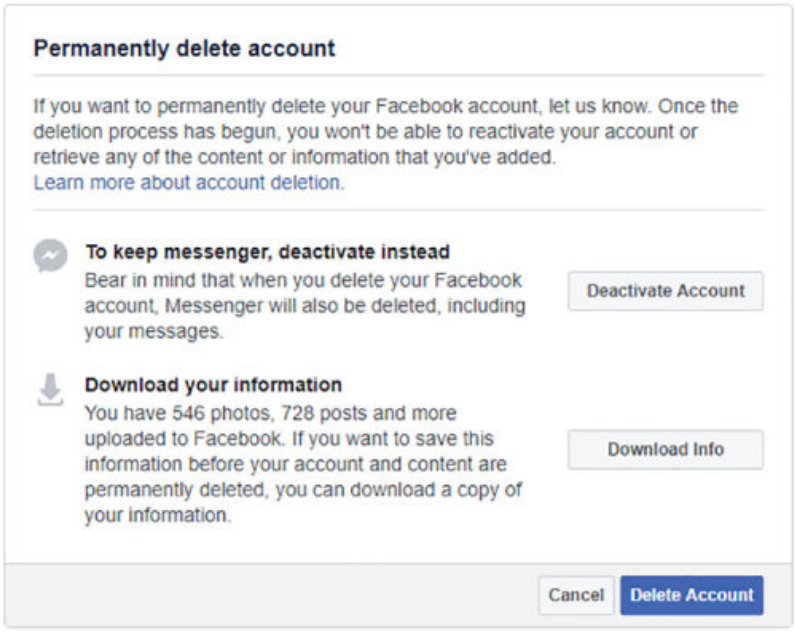



Screenshot: Gizmodo

Choose **Disk Utility** from the list of options, then select the drive holding the operating system and files on your computer. Click **Erase** at the top, select **Mac OS Extended (Journaled)**, when prompted, then click **Erase** again. After the process has been completed, you can choose to reinstall macOS or leave it for the next user (hit **Cmd+Q** then **Shut Down** to turn the Mac off).

## Your web accounts

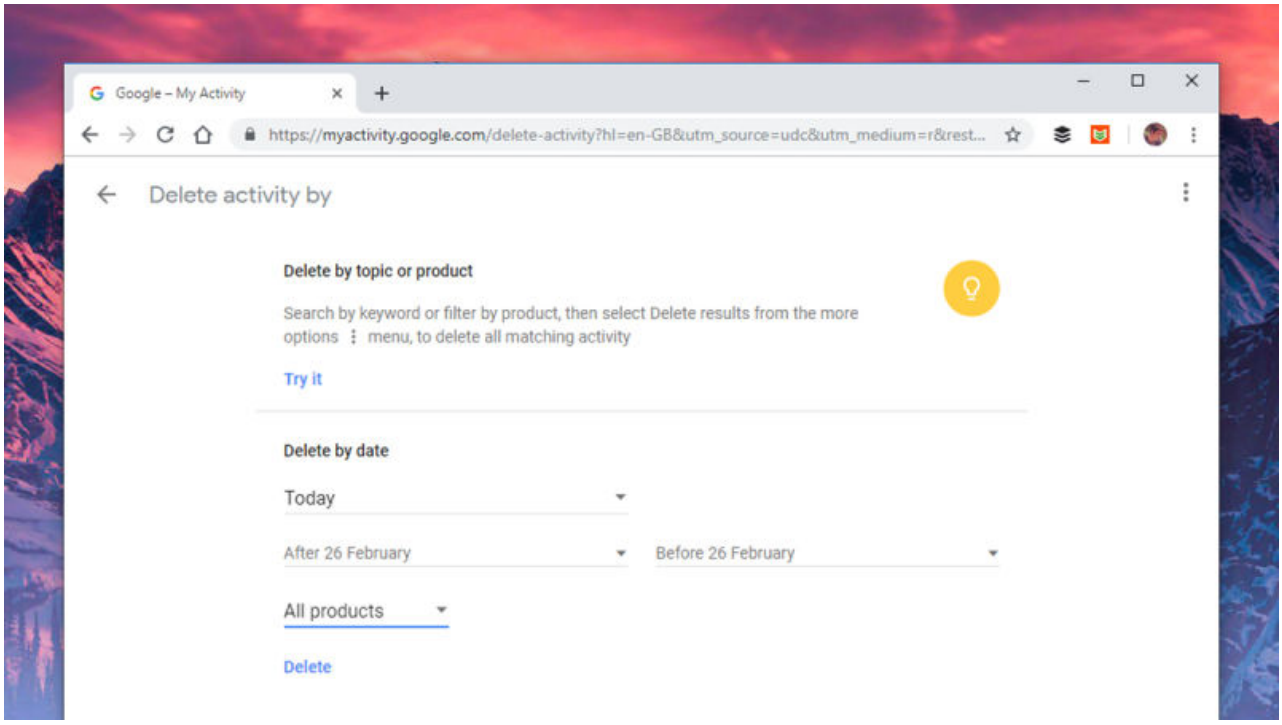
We can't go through every web account you might have signed up for but we can give you some pointers for the main ones. Your options are going to vary from service to service. For example, it can take up to 90 days to delete all your data past the point you've decided to get rid of your account.




Screenshot: Gizmodo

If you want to wipe your Facebook account, open the Settings page on the web, then click , **Delete your account and information**, and **Delete Account** (taking advantage of the data export options listed if you want to use them). If you want to keep using Facebook Messenger, choose **Deactivate Account**, but your personal data won't be erased—just hidden.

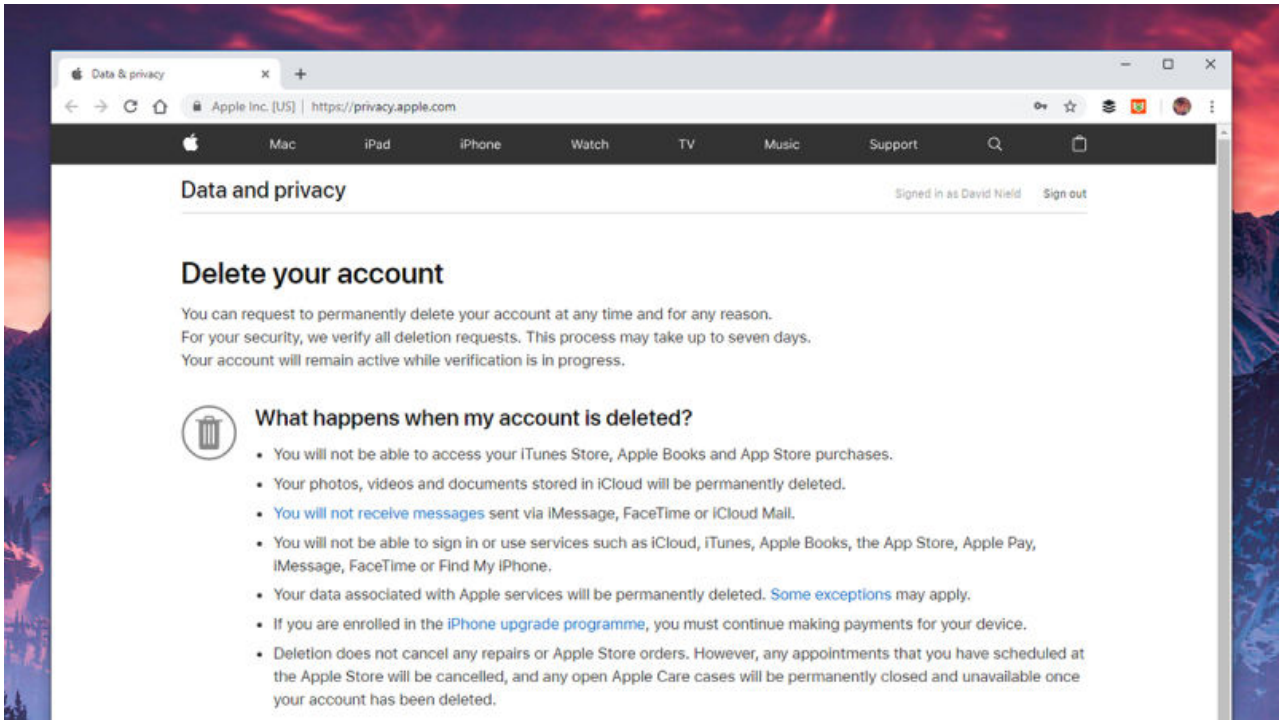
The process is similarly straightforward on Twitter: Go to the Settings page in your browser, then choose **Deactivate your account**. Enter your password, confirm your choice, and you're done—you can get your account back for up to 30 days afterward, but after that, it's gone forever. Remember to export your tweets if you want to save them.




Screenshot: Gizmodo

Various third-party services will delete a subsection of Facebook posts or Twitter tweets for you, but considering their reliability and privacy standards can be suspect, we find it difficult to recommend them—use one of these tools at your own risk.

Google keeps a whole stack of data on you, and the Activity controls page online is your way into erasing some or all of it from existence. Use the toggle switches to stop logging data in the future, or one of the **My activity** links to delete it—if you then choose **Delete activity by**, you can wipe recorded data by date and Google service. If you want copies first, go to .




Screenshot: Apple

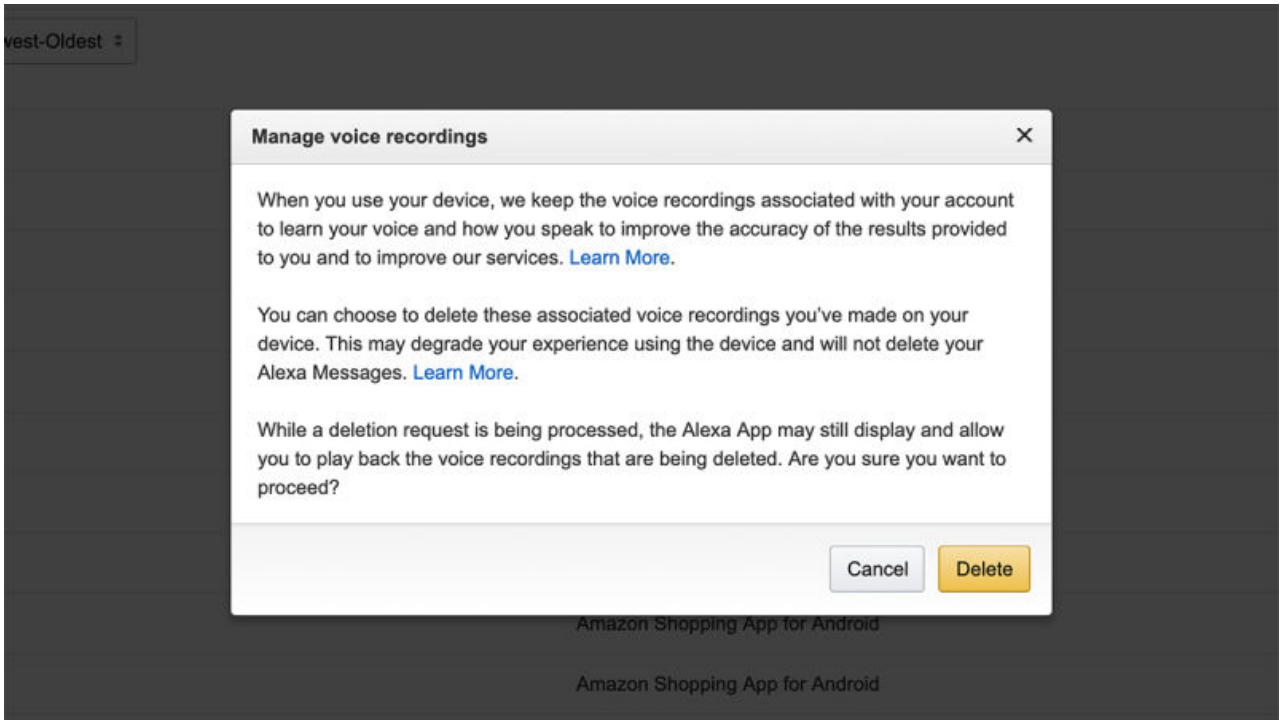


Sometimes it's easier just to go into the Google app or service in question. In Gmail click **All Mail** on the left, then the selection box in the top left corner above your most recent email. Choose **Select all…** (which will tell you how many messages are in your Gmail account), then click the **Delete** icon to send them to Trash. The emails will stick around for 30 days unless you click **Trash** and **Empty Trash now**.

Want to go nuclear on everything Apple has on you? iTunes purchases, calendar entries, iCloud emails, iCloud photos? Well, Apple will let you do it if you go to this page on the web: Once you've signed in, click **Request to delete your account**, read through the information, and confirm your choice at the bottom.

## Your other activity

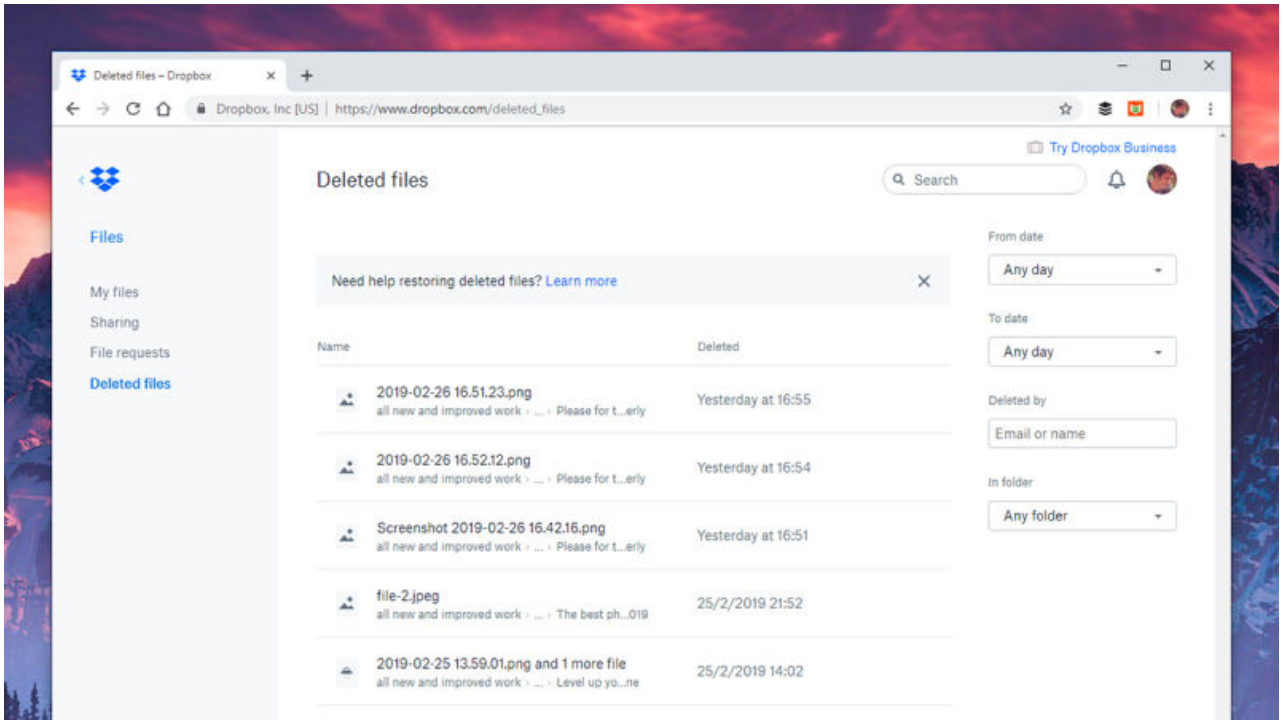
Your data is floating around in all kinds of places you might not think about. If you're ditching your smart speaker, why not delete everything you've said to Alexa at the same time? From this device page on the web, click the button to the left of your Echo, then choose **Manage voice recordings** and **Delete**.




Screenshot: Gizmodo

Most cloud storage services worth their monthly fee will keep deleted files around for a while in case you suddenly find you need them back—great if you've made a mistake, not so great if someone else gets access to your account or computer and pulls back a few files from their digital graves. If there's something sensitive you really want wiped, make sure that it really is wiped.

Whenever you're deleting any web accounts, it's also a good idea to pull any third-party apps linking into them too, because your data could be replicated elsewhere. You can find the list for your Facebook account here, for example, and the list for your Google account here. Not all of these will have access to personal data, but some might.




Screenshot: Gizmodo

What else might you be leaving behind without realizing it? You'll find that properly and securely deleting data and accounts only takes a little longer than just leaving them to gather (digital dust). It's well worth that extra effort to protect any data leaking out that shouldn't.

## Do more with your data