SHRINK YOUR ONLINE FOOTPRINT

You're almost certainly leaking more information online than you realise. Nik Rawlinson reveals the dangers of sharing, and the steps you can take to downsize your online footprint

We're the over-sharing generation. You might think that your Facebook posts, Twitter missives and LinkedIn musings are all suitably considered and circumspect, but over time your accumulated posts will inevitably build up a picture of who you are – perhaps including where you live, what you do for a living, your childhood, your family composition, birthday and more. All of which would be valuable information to a potential identity thief.

As an example, let's say you post a picture of your child blowing out candles on a cake. Unless the metadata has been stripped first, you've probably also shared the date on which the picture was taken. If your child is young, it's unlikely they waited until the weekend to celebrate, so there's a good chance the date it was taken was their birthday itself, even if you didn't post it until a few days later. If there are three candles on the cake, or a card with a number on it, that's the other half of the equation: anyone stumbling on your post now knows exactly when your child was born. If you've used their birthday – or part of it – in a password or security question, that's a chink in your digital armour right there, ripe for exploitation.

That's not the worst of it. If you took the picture on your phone, the exact coordinates of the place where it was taken could be embedded into the metadata. That's probably your home address, so anyone who sees the picture immediately knows exactly where to find that nice painting hanging in the background. If you're a married woman and your friends list includes family members, it won't be hard to deduce your maiden name – another common security question. The list goes on. Photos of your first car, connections to school friends... every seemingly innocuous detail makes you more vulnerable to exploits and scams.

Now consider the data you've scattered outside of social networks – the CVs you've uploaded to job sites, the links you've stored in a cloud-based bookmarking tool, ads you've clicked on, the emails you've received in a webmail inbox and the places you've been with your phone in your pocket.

You'll never get rid of all this data, whether it escaped through active over-sharing or was collected without you noticing. What you can do is take stock every so often, audit your digital footprint and shrink it where you can – and the obvious place to start is social media.

SHRINK YOUR FACEBOOK FOOTPRINT

To find out what information Facebook is holding about you, log in through a browser and click the down arrow in the top-right corner.

Click "Settings & privacy", followed by Settings. Select "Your Facebook information" in the sidebar, then "Download your information". Leave the default settings as they are and click "Create file". It will take a short while for Facebook to collect the applicable information. When it's finished, you'll be able to download a ZIP file, whose contents you can peruse to see what's stored against your name on Facebook's servers. Armed with this data, you can decide what stays – and what should be removed.

Deleting content from Facebook is surprisingly easy, especially if you use the Manage Activity tool; this lets you remove batches of information at a time, rather than just individual items. The catch is, it's currently only available in the Facebook mobile app. To access it, tap the menu button on the toolbar, then hit "Settings & privacy", followed by Settings. Now select "Activity log"; to remove individual entries, tap the three dots on the right of the screen beside each one. To delete several entries at once, tap "Manage activity" and pick whether you want to manage posts, activity you're tagged in or interactions such as likes, reactions and comments.

Whichever you choose, Facebook will pull up a list of the ten most recent data points, and scrolling down the screen will extend the list. Tap the box beside each item you want to remove, or tap the box at the top of the list to select everything that's shown on the page (you might want to scroll down to extend the list a few times). Finally, tap the remove or recycle button – depending on what you're deleting – at the bottom of the screen.

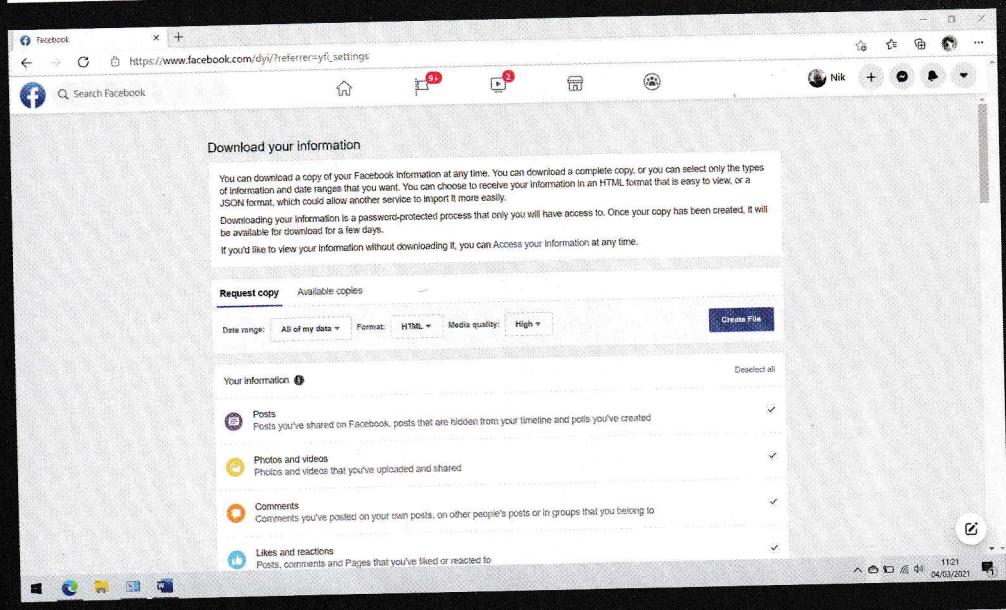
If it's not convenient for you to use the Facebook app, you can also delete content through the browser – it's just more time consuming. Log in and click the down arrow at the top of the screen, followed by "Settings and privacy" and Settings. Click "Your Facebook information", followed by "Activity log". As you hover over each item in the sidebar, three dots will appear on top of it, allowing you to unlike things you have liked or move content you've posted to the archive or recycle bin.

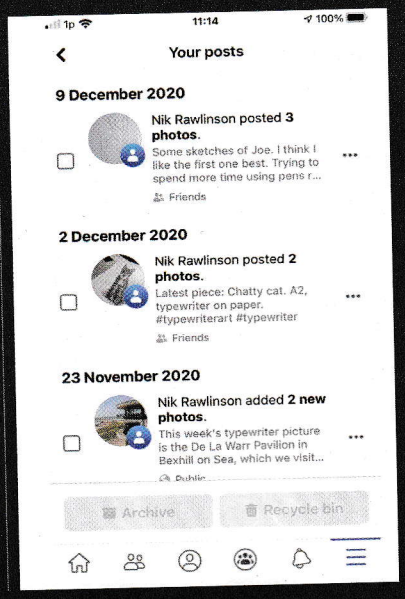
While these functions let you manage your publicly accessible content, you should be aware that Facebook also collects data to make decisions about what to show you. To review this, select "Privacy shortcuts" from the "Settings & privacy" menu and then "Review your ad preferences" (in the "Ad preferences" box) or "Manage your information" (in the "Your Facebook information" box).

If you're reviewing your ad preferences, click "Ad settings" in the sidebar and work your way through each of the sections in the "Manage data used to show you ads" section. Some of the settings you'll find here let you prevent advertisers from reaching you on third-party websites based on your Facebook data, while others let you see the content categories Facebook thinks you're interested in.

This latter information can be quite eye-opening. It's not always spot-on: I discovered that I was being targeted for content related to *Assassin's Creed*, even though I haven't played a computer game in more than 20 years. For the most part, though, the list was scarily accurate (it even knew the brand of watch I wear). There are links on the page that let you remove any categories that don't apply, or which you'd simply prefer Facebook not to use for targeting.

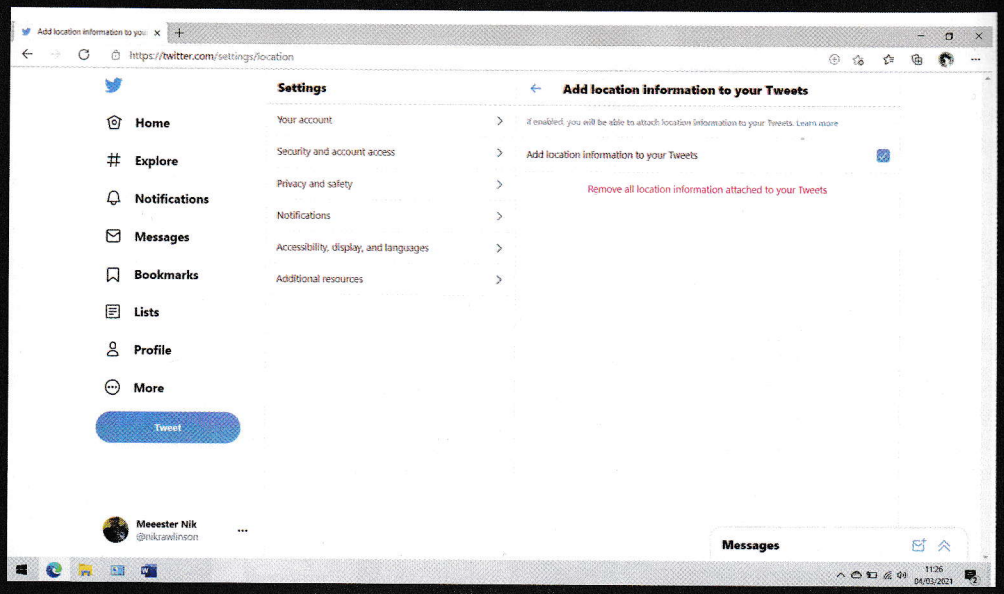
If you want to get off Facebook altogether, the "Manage your information" section provides links to delete your data and close your account. If you're hesitant about leaving the platform because you don't want to lose touch with friends or family members who are using Facebook Messenger, there's good news; it is possible to continue





BELOW As with any social network, it makes sense to first download your data

BELOW RIGHT The easiest way to delete Facebook data is via the app



using Messenger for instant messages even after deactivating your main Facebook account – see **pcpro.link/320messenger**.

If you decide to take the plunge, point your browser at **facebook.com/deactivate**, enter your password, complete the form and click Deactivate.

INSTAGRAM

You might imagine that Facebook-owned Instagram would offer similar levels of control over your content. Sadly, that's not the case: you can discover a lot about the metrics that are used to determine what you're shown in the app, but you can't always correct or delete any incorrect inferences.

To see what Instagram thinks of you, open the app and tap your icon at the end of the toolbar, followed by the three lines at the top of the next page. Tap Settings followed by "Ads | Ad topics" and untick subjects that don't interest you. If you tap into Security, rather than Ads, and hit "Access data", you can see your apparent interests in blocks by selecting "View all" under "Ad interests" – but you can't delete items recorded here.

You can, however, flag unwanted adverts individually. Tap the three dots above them in your feed then tap "Hide ad". You can specify whether the ad is irrelevant, shown too often or inappropriate.

LEFT You can choose to turn off selected topics for ads in Instagram

ABOVE Removing location data will stop people seeing where you tweeted

SHRINK YOUR TWITTER FOOTPRINT

To find our what Twitter knows about you, log in through a browser and click More in the sidebar, followed by "Settings and privacy". As with Facebook, the information is provided as a bulk download: with "Your account" selected in the second sidebar, click "Download an archive of your data" in the third, and enter your password. Click the "Request archive" button and Twitter will compile a Zip file. It will send you an email when it's ready for collection.

Once you know what kind of information the database holds about you, you can make more informed decisions going forward. In the meantime, there are some specific settings that it's worth looking at (all of the menu options mentioned below are found under the "Privacy and safety" section of Twitter's settings).

If you want to restrict your tweets so they can be read only by people who actively follow you, click "Audience and tagging" and click the box beside "Protect your tweets". While you're in this section, you can optionally disable photo tagging too, which stops people identifying you in photos they post to their own profiles. Once you've protected your tweets, you'll be asked to authorise any future follower requests, rather than allowing anyone who wishes to follow you do so.

A specific privacy issue that we mentioned earlier is the possibility of giving away your whereabouts. To prevent Twitter from reporting your location, click "Your tweets", then "Add location information to your tweets". Untick the box and, optionally, click the link to wipe

FORTUNATELY, GOOGLE HAS GREATLY SIMPLIFIED THE TASK OF KEEPING EVERYTHING UNDER CONTROL

location data from tweets you've posted in the past.

Again, like Facebook, Twitter builds up an internal profile of you that's used to select ads and suggested content. You can review this, and remove specific interests from your record as you wish. To do so, click "Content you see | Interests" and untick the box for each subject you'd rather not hear about.

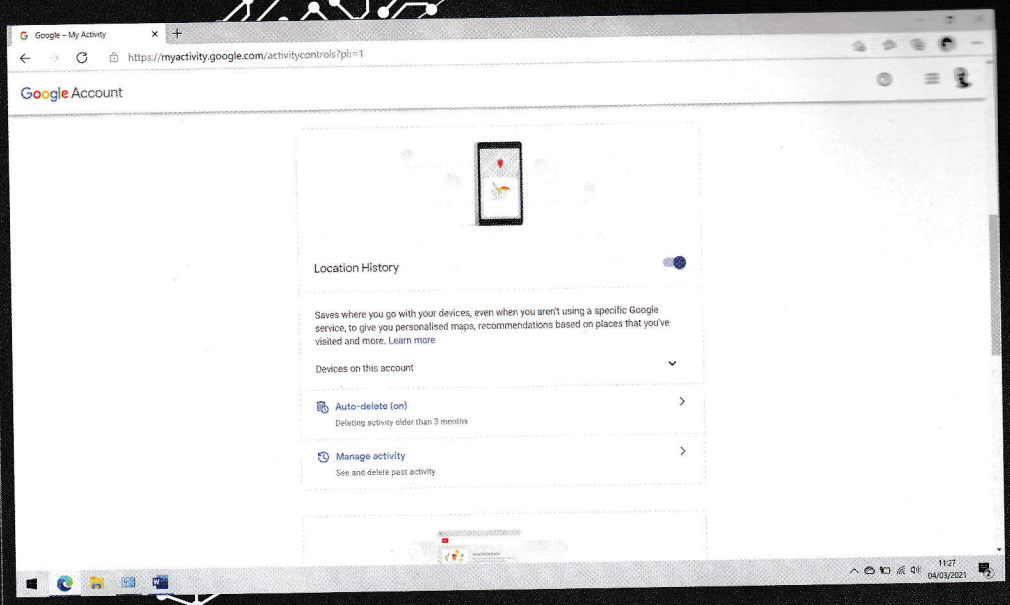
As for items you've actively shared, it's easy to delete individual tweets by clicking the three dots icon on each one and selecting "Delete tweet". Twitter doesn't provide any way to remove whole batches of posts, but a number of third-party services have sprung up to plug the gap. Check out **tweetdeleter.com**, **twitwipe.com**, or **tweeteraser.com**. If you want to go the whole hog and delete your Twitter account, point your browser at **twitter.com/settings/deactivate**.

SHRINK YOUR GOOGLE FOOTPRINT

Google offers an extraordinary range of products and services, many of which collect a whole lot of personal information – either for publication or for internal usage. Fortunately, the company also provides a single centralised dashboard from which you can keep track of everything that's being stored about you across Google's numerous sites and apps. To access it, start by navigating to **myaccount.google.com** and logging in.

Once you're authenticated, a good place to begin is **myactivity.google.com/activitycontrols**. Here you'll find options to turn off whole categories of data collection, including location data, data gathered by Google-owned websites and Chrome, and data collected by devices such as your phone and tablet. You can also limit what information is collected and used by YouTube: this will probably cause you to receive less relevant video recommendations, but you may not consider that a great price to pay for enhanced privacy.

At the bottom of the page there's also a link to the advertising settings page at **adssettings.google.com**. If you want to see random ads, rather than ones based on your behaviour, just click off the switch labelled "Ad personalisation". This only affects advertising on Google sites, but if you visit the Your Online Choices website at **pcpro.link/320choices**, then you can similarly turn off advert personalisation for dozens of different companies.



ABOVE Google's privacy controls let you switch off its data collection

If you want to remove your own content from your Google account – such as contacts, calendars, Drive data, ebooks, Play store purchases and so forth – it's a good idea to download an archive of your content in advance, just as with Facebook and Twitter, which you can do from **myaccount.google.com/dashboard**. When you visit the page you'll see a long list of all the Google services that your identity is connected to; to download data for any of these individual services, click the down arrow to expand it, then click the three dots at the bottom of its card, followed by "Download data". Clicking the main "Download your data" link at the top of the page will download a complete archive of content from all the various services.

Bear in mind that this page only shows and retrieves information for

VOICE ASSISTANTS

If you're concerned about what your voice assistant might be recording, you can take charge of this just like any other sort of personal data. The Google Assistant doesn't save your audio by default, but you can optionally enable the capability at **pcpro.link/320activity**. While there, you might want to click the "Auto-delete" option and set your data to be wiped after three, 18 or 36 months.

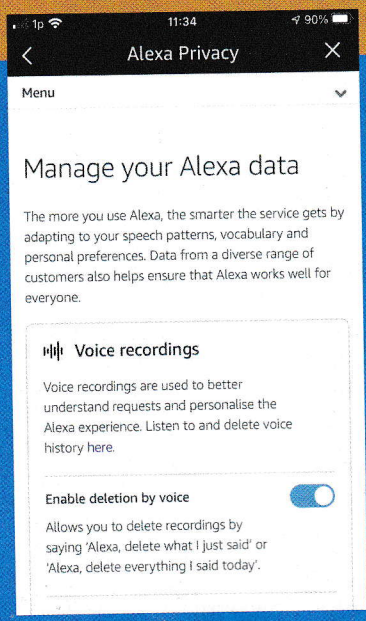
If you want to see if your Assistant devices have captured any recordings, go to **myaccount.google.com/yourdata/assistant** and check the settings under Google-wide controls. Under "Audio recordings", select "Listen to and delete activity".

If you have an Amazon Echo device, you can use your voice to instruct it to "delete all of my voice recordings". You'll be warned that this might make it harder for Alexa to respond to your requests, and will then be asked to confirm the deletion. If you just want to delete anything picked up in the last ten minutes, say "Alexa, delete my voice recordings".

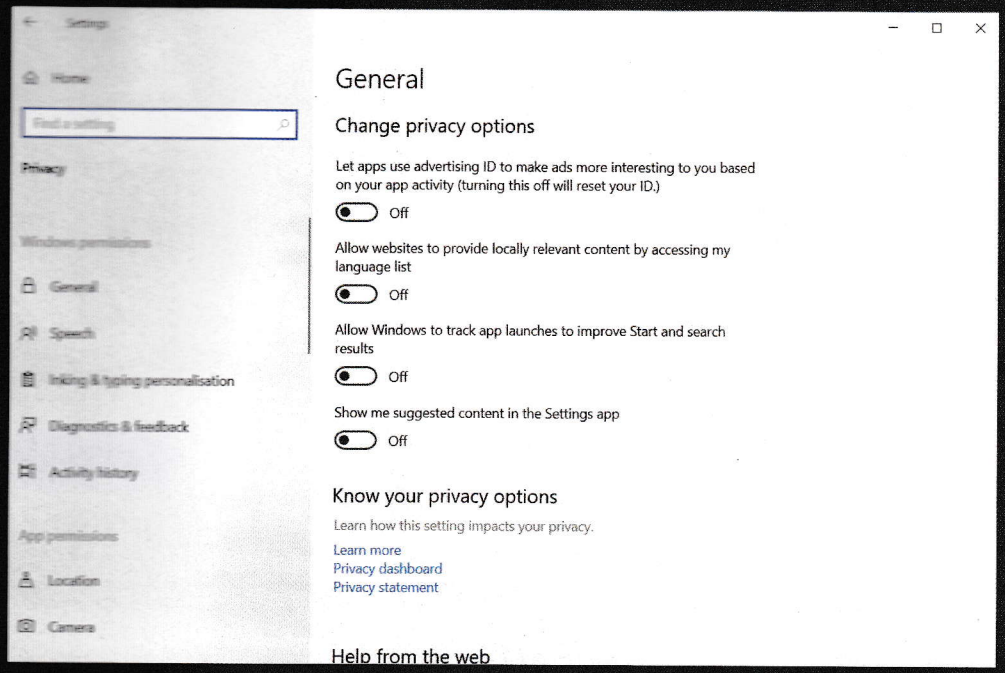
If this doesn't work, make sure deletion by voice is enabled in your account. Open the Alexa app on your phone and tap Settings | Alexa privacy. Tap "Manage your Alexa data", then make sure the switch beside "Enable deletion by voice" is on (to the right). The row below this lets you specify how long Alexa retains recordings; by default, they're kept until you delete them, but you can switch this to three or 18 months, or disable recording altogether.

To do the same with Cortana, log in to your Microsoft account at **account.microsoft.com**, then click Privacy at the top of the page. Scroll to "Voice activity" and click "View and clear voice activity".

Finally, to delete recordings and other Siri-related data on an iPhone, iPad or iPod Touch, open Settings | Siri & search | Siri & dictation history. Then tap "Delete Siri & dictation history".



RIGHT You can delete your Echo data using your voice, as long as the feature is enabled



the currently logged-in Google account. If you have multiple accounts – one for work and a personal account, for instance – you'll need to repeat this process for each one. You can keep track of which identity you're using by checking the account image at the top right of the dashboard pages.

SHRINK YOUR MICROSOFT FOOTPRINT

Like Google, Microsoft has helpfully centralised a lot of its privacy settings in a unified dashboard, which you'll find at **account.microsoft.com/privacy**. You can download a copy of your activity by clicking "Download your data", followed by "Create new archive". The resulting file will include things like your search and location history and other personal information, but it won't include data generated in applications such as Office Online or the Outlook calendar. To download those items, you'll need to go into each product and manually make a copy of whatever you want to keep.

One information repository that's of particular interest is what's known as Cortana's Notebook, which is where Cortana keeps track of things it's learned about you, to help it provide relevant answers to any questions. You'll find a link to this at the top of the Privacy page, with the data broken into sections covering topics such as your commute, weather preferences, news stories that interest you, stocks you're tracking and so on. The more information Cortana has squirrelled away, the more effective it will be – but, if you'd rather wipe what it knows, click "Clear Cortana data" in the right-hand sidebar.

Like Facebook and Google, Microsoft also provides an easy way to opt out of so-called behavioural advertising, which by default serves up content based on what it knows about you. To do so, visit **account.microsoft.com/privacy/ad-settings** and turn off all of the switches for personalisation.

Don't forget to also check your privacy settings in Windows itself. Press Windows+I to open the Settings app and click Privacy, then use the switches to manage what the operating system can and can't do. The standard settings allow the OS to show ads based on your interests and websites to access your language lists to provide locally relevant content, but these can be turned off at the flick of a switch. You can use the App permissions link at the left to block third-party apps from accessing information such as your location and account settings too.

ABOVE Microsoft's privacy dashboard is accessible and comprehensive

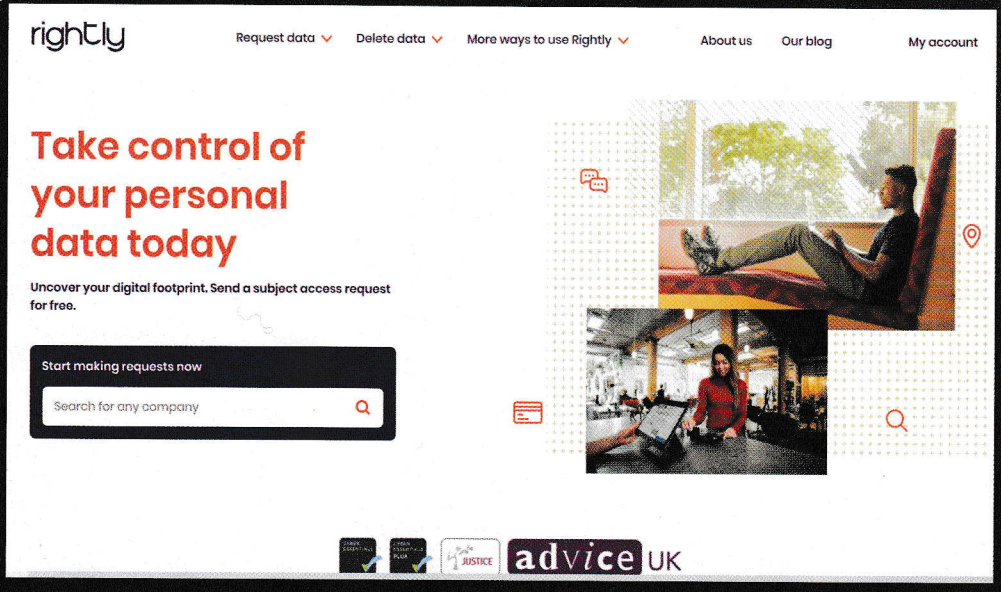
PREVENTION IS BETTER THAN CURE

The companies we've focused on have huge databases of personal information, but don't think your digital footprint stops there. It also extends to, for instance, the online supermarket that brings your groceries, the public library you use to download ebooks, your favourite digital magazine stores and anywhere you've ever saved your credit card details.

To audit and curate exactly what all of these services know about you can be a time-consuming business. However, it's made a lot easier by services such as Rightly (**rightly.co.uk**), which provides direct links to all manner of companies, with options to see what information they hold about you, to opt out of marketing or to request deletion.

It's also important to realise that even if you take direct action, close your accounts and request that companies scrub you from their databases, your information may still be out there somewhere. The things you publish online can easily find their way into various archives operated by an incalculable number of third-party services, without your ever knowing about it.

The only truly safe course of action, therefore, is never to publish anything that you might regret sharing in the future. That might not be realistic, so the next best option is to lock down any services you actively use from the very start, to prevent them from gathering personally identifiable information in the first place.



BELOW Rightly can help you remove data from third-party services