8 Steps to Secure Your Facebook Privacy Settings

WRITTEN BY: JULIANNE SUBIA

JANUARY 13, 2019

Facebook's privacy settings have recently undergone a massive change since Facebook's privacy scandals have been in the news. The most recent change was implemented in response to the Cambridge Analytica scandal, where the political consulting firm improperly used the data of roughly **87 million** Facebook users while working for Donald Trump's election campaign.

Since the scandal broke, Facebook users have made an effort to improve their privacy. According to the **Pew Research Center**, more than half of users have changed their privacy settings in the six months directly following the scandal. Additionally, four out

of 10 users have taken a break from Facebook, and 25% of users deleted the Facebook app from their smartphone.

Here are some easy but significant changes to make in your Facebook privacy settings to help you take control of your account.

1. Remove Personal Information

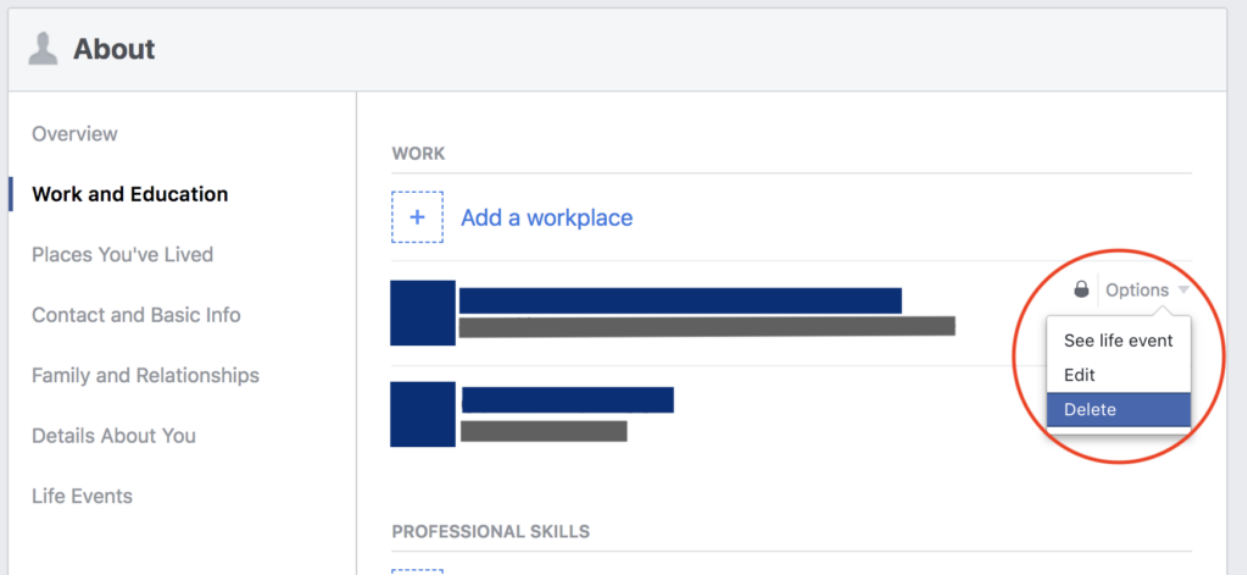
When you signed up for Facebook, you were prompted to fill out your profile with information like your phone number, hometown, what school you went to, etc. You might have added all of this without thinking too much about it, or thinking that it might help friends find you.

Instead, people can use this information to steal your identity. For example, it's easy for a hacker to figure out your high school mascot if your high school is right there on your profile, and then fill out security questions to hack into your bank account. It's also possible that Facebook filled in this information based on your photos and posts, without you entering it in yourself.

Remove this information in your Facebook privacy settings by going to your profile and clicking "About", underneath your name and timeline photo. Work your way through each section until your information is deleted.

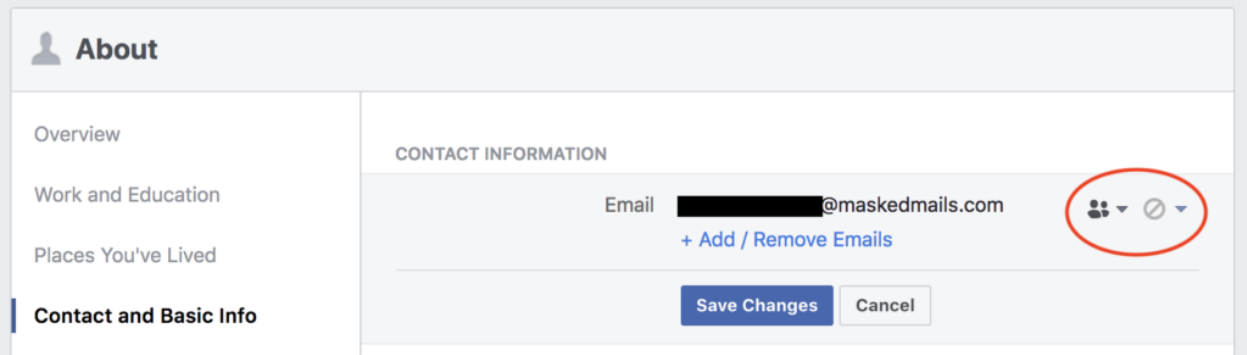
Screenshot taken by Julianne Subia/Abine.

When you click on each section on the left, you will be able to delete each piece of information by clicking on ‘options’ next to the lock picture on the right.



Screenshot taken by Julianne Subia/Abine.

You also probably used your real email address when you signed up, and maybe also your phone number. When you use your real email and phone number, Facebook and advertisers can connect your account to your email and other accounts. Replace your email on Facebook with a **‘masked’ email address** from Blur. Then, change your Facebook password with **a strong password** generated by Blur. If you’re using repeat passwords for different accounts, it’s easier for hackers to guess them. By using a unique strong password for each site, you protect yourself from this kind of guesswork. And don’t worry, Blur has a password manager service to help you keep track!



Screenshot taken by Julianne Subia/Abine.

You should also make sure that your email is limited to Friends and hidden from your Timeline – this way, nobody can see it.

2. Control who can see your information

First, you will want to go through your friends list and make sure that you know everyone there. Remember, these people can see everything that you post, so make sure that you have a reasonable level of trust with them. Be on the lookout for **bot** and **impostor** accounts sending you friend requests.

On your Facebook profile to the right of your name, click ‘View As’. This will allow you to see what is public on your profile- i.e. what a person would see if they were not your ‘Friend’. This will allow you to make sure that you are not sharing anything publicly that you don’t want to.

Screenshot taken by Julianne Subia/Abine.

3. Limit Your Audience in Facebook Privacy Settings

Go to your **Facebook Privacy Shortcuts** and click “See more privacy settings” at the bottom of the first list.

Here, you can make sure that only people you know can see your posts. First, make sure that only Friends can see your future posts (the top line). Next, make sure that your only Friends can see your past posts by clicking “Limit Past Posts”.

You can reduce unwanted friend requests by making sure that only ‘Friends of friends’ may contact you (the fourth line).

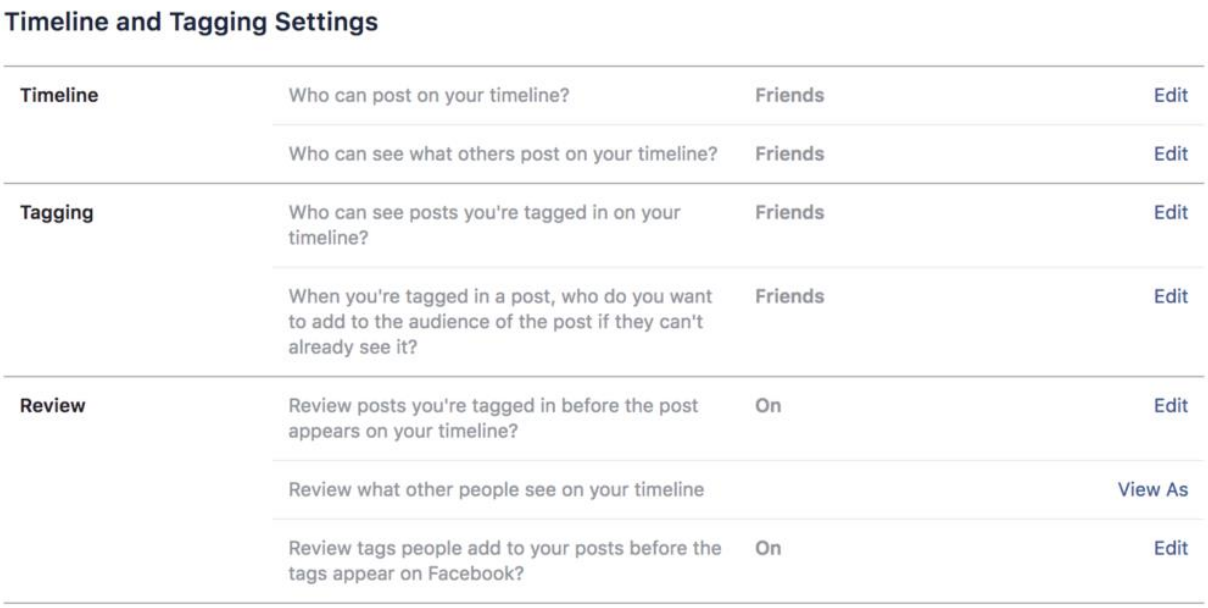
Privacy Settings and Tools

Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How People Find and Contact You	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list?	Friends	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

Screenshot taken by Julianne Subia/Abine.

4. Control Tagging

From the privacy shortcuts page in the left bar, click on 'Timeline and Tagging'. Make sure that only 'Friends' can post and see things that others have posted on your Timeline. You will also want to make sure that only Friends can see things that you've been 'tagged' in, i.e., something that somebody else has posted about you. Add an extra layer of security by turning on 'Review'- this way, you will be able to review something that a friend has tagged you in, before it shows up on your Timeline.



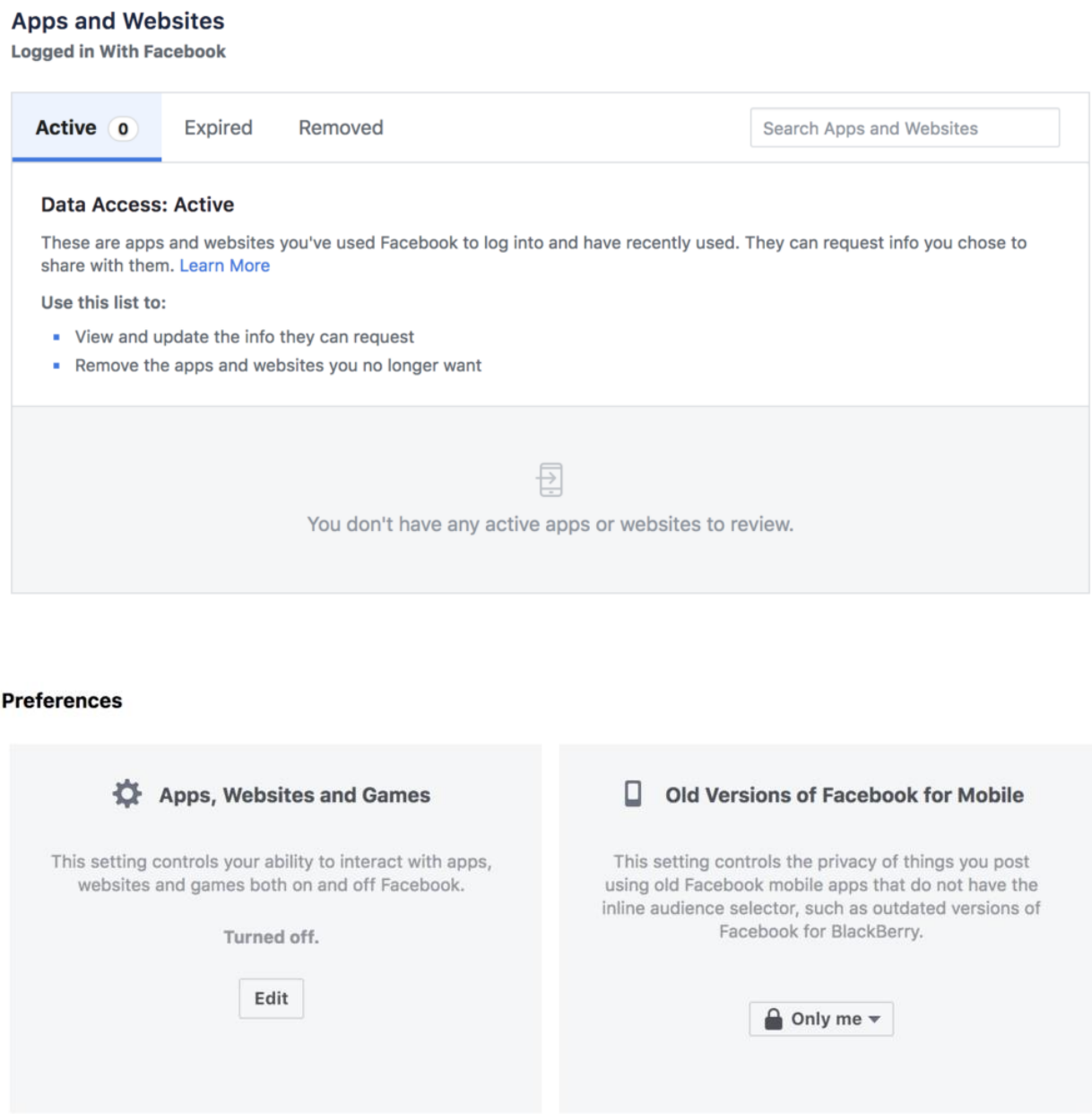
Timeline and Tagging Settings

Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
Tagging	Who can see posts you're tagged in on your timeline?	Friends	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Friends	Edit
Review	Review posts you're tagged in before the post appears on your timeline?	On	Edit
	Review what other people see on your timeline		View As
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

Screenshot taken by Julianne Subia/Abine.

5. Remove Access to Third-Party Apps

You've probably noticed that you are often offered the ability to 'Login with Facebook" when logging in to apps like Spotify or Instagram. This might be convenient, but it also lets these apps see your Facebook information- like your birthday, friends list, and other things they don't need to know. Go to the **Apps and Websites section** of your privacy settings and remove any apps or sites that you're not using or security that you don't trust.

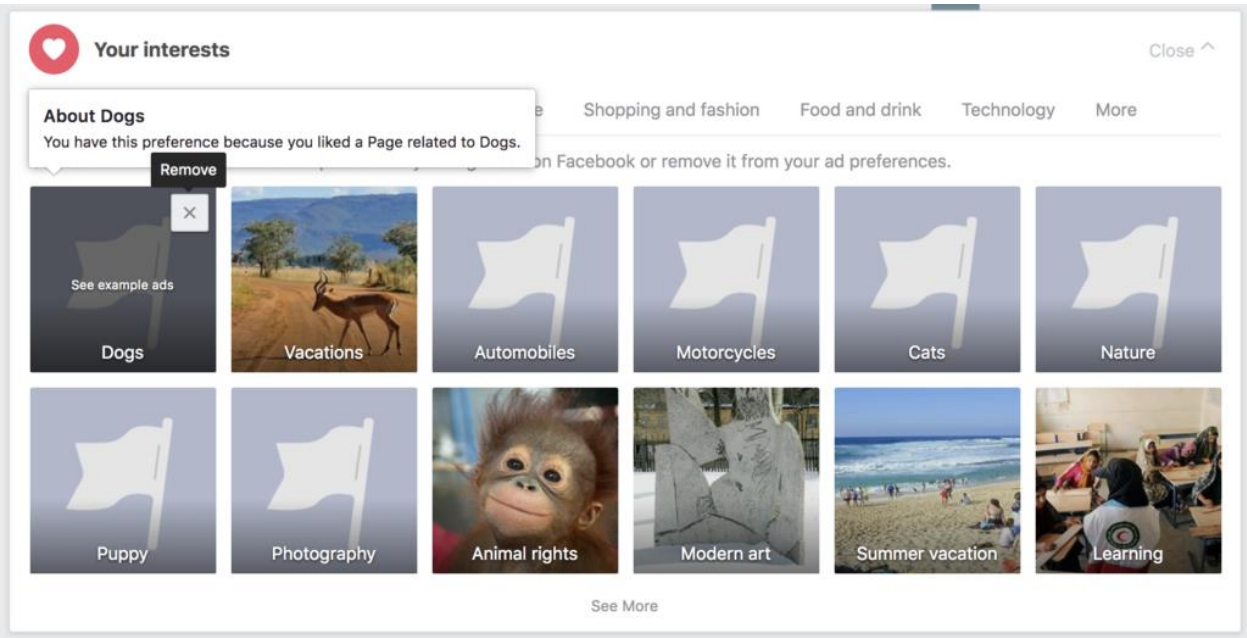


Screenshot taken by Julianne Subia.

6. Opt-Out of Interest-Based Ads

Go to your **Facebook ad preferences** and go through each section. Pay special attention to the sections “Advertisers You’ve Interacted With,” “Your Information,” and “Ad

Settings". In "Your Information," you can disable information that's shared with advertisers, including your relationship status, employer, job title, and education.

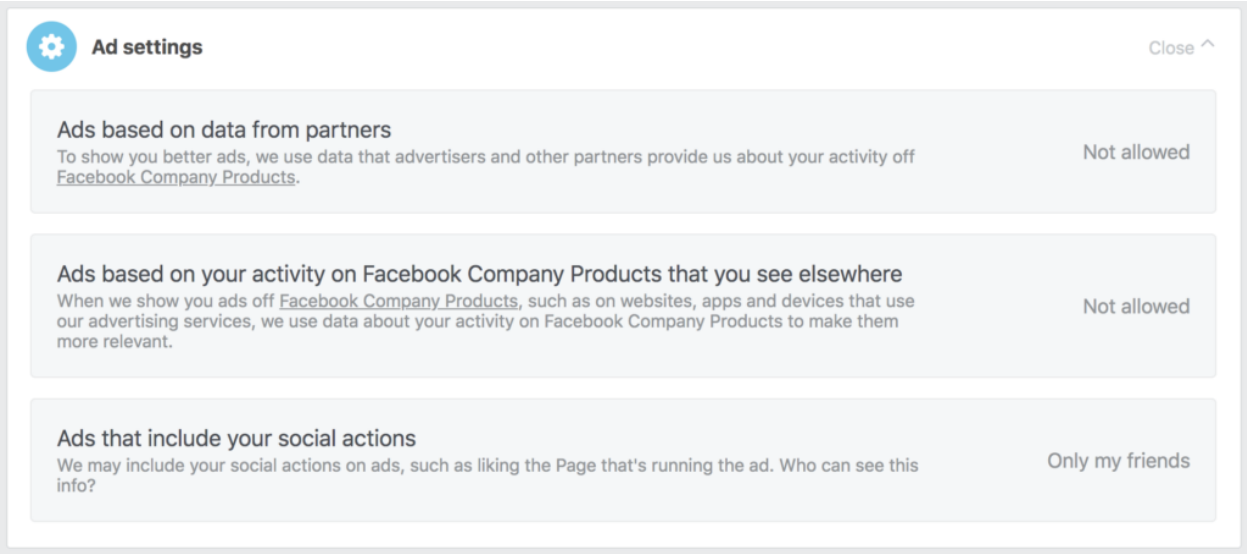


Screenshot taken by Julianne Subia.

There are three options under "Ad Settings":

1. **"Ads based on data from partners":** This is how Facebook tailors ads to you, based on your activity off of Facebook. For example, you might have noticed how after looking at a certain coat on Amazon, you see ads for it on Facebook. To stop seeing ads like this, click "not allowed".
2. **"Ads based on your activity on Facebook Company Products that you see elsewhere":** Facebook and its "Company Products", such as Instagram, share information about your activity with outside advertisers. For example, if you read an article about the best smartphone on Facebook, that can be shared so you'll see ads for smartphones elsewhere online. To stop seeing ads like this, click "not allowed".

3. **“Ads that include your social actions”:** With this setting on, your friends might see ads with a line “Jen liked this X Company”, or “Jack has been to Y Restaurant”. Click “no one” in this setting to stop your friends from seeing your interactions with ads.



Screenshot taken by Julianne Subia.

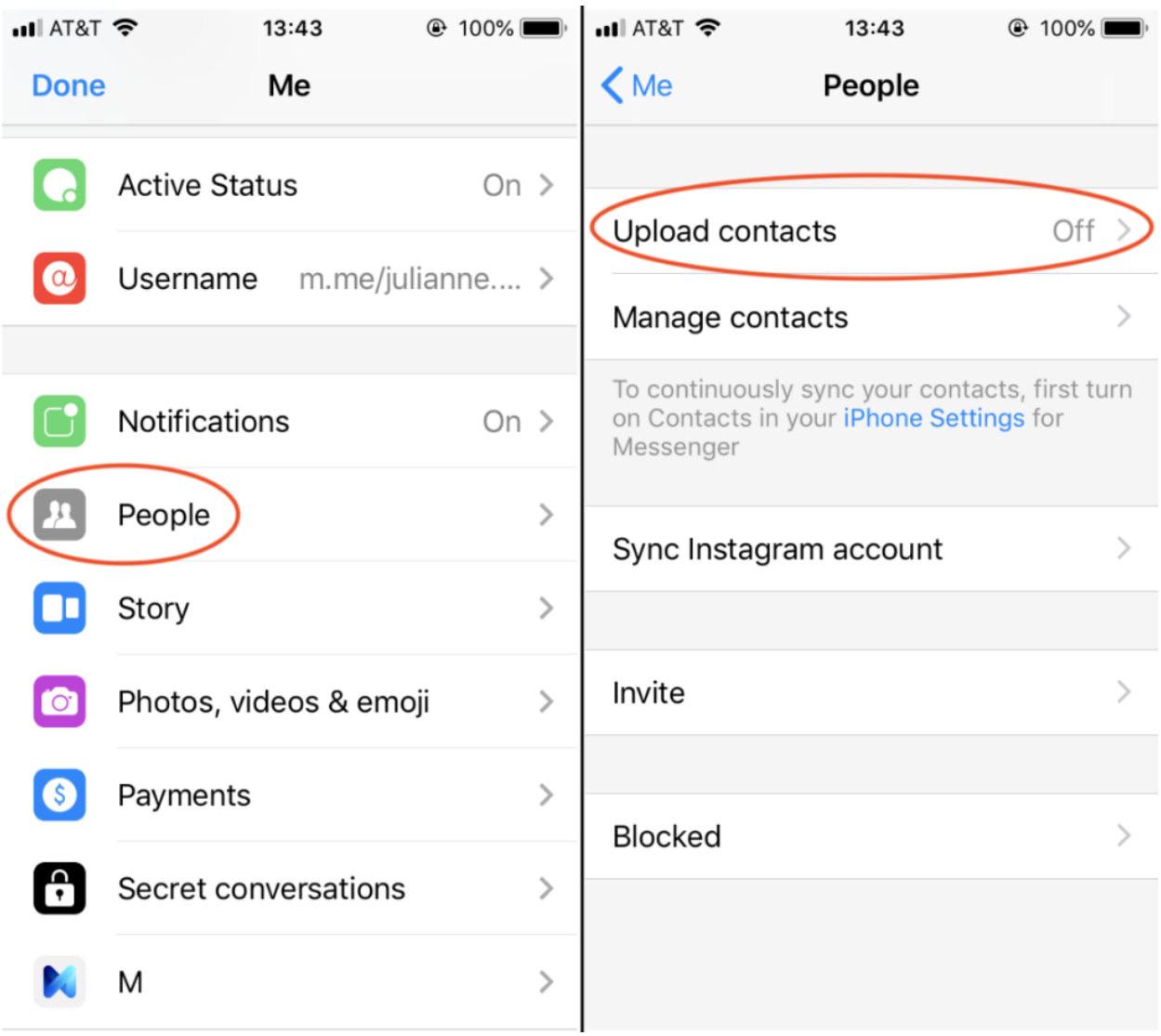
7. Remove Your Activity Data

You can edit your activity record so Facebook will no longer have a detailed log of your account activity. Go to your **activity log** and delete unwanted record.

Pro tip: use the **Social Book Post Manager** extension on Google Chrome to automate the process. Your posts won’t be actually deleted, but Facebook will no longer have a detailed log of your activity.

8. Protect Yourself on Messenger

If you have your contacts synced on your Facebook Messenger app, Facebook might have access to your call and text message history. To turn this off, go to messenger and click on your profile picture on the top left. Then click 'People' in the menu, and turn of Upload Contacts'.



Screenshot by Julianne Subia/Abine.

Facebook Privacy Settings Can Keep You Safe

We rely on Facebook for so many things – staying in touch with friends, finding events in our communities, or even networking to find jobs or roommates. These tips can help you stay safe, without giving up your Facebook account. Your privacy is just that, ***yours.*** You shouldn't have to give away all of your personal data just because a company suggests that you should.

Finally, if you just want to delete your Facebook account, check out our **how-to post** for step-by-step instructions.

About the Author / Julianne Subia

Julianne Subia joined Abine's Marketing Team in 2018. Julianne has a degree in International Justice from Leiden University, and focuses on Privacy from a Human Rights approach.

About Abine

Abine, Inc. is The Online Privacy Company. Founded in 2009 by MIT engineers and financial experts, Abine's mission is to provide easy-to-use online privacy tools and services to everybody who wants them. Abine's tools are built for consumers to help them control the personal information companies, third parties, and other people see about them online.