Social Media

We recommend careful practices around social media. Consider not just what information you may feel is compromising to you, but what may be compromising to your friends identities or projects, even when it just gives adversaries a place to start looking. We see a large amount of doxxing targeting happening through social mapping and we know the state does the same. When you have an adversary who will look through every one of your 1000 friends to see if they recognize a picture, full security becomes more important.

Ask yourself what you're getting out of a given social media platform and adjust accordingly. Barely use it? Consider getting rid of it. Even if you use it actively, there may be a lot of old information and photos that don't impact your utility but do present a liability. If you delete an account, update your password security and your recovery accounts/logins before you do so – don't give adversaries an opening to "recover" it as you. If you choose to have a continued account, we recommend not attaching your name or your legal name to it and ideally not attaching an alias that's used anywhere else as well as not using a picture that shows identifying information.

Facebook:

- Account removal:
  - To deactivate, understand that though you will be able to access it later, it is also vulnerable to hacks, subpoenas, etc. Go to account settings -> manage accounts and hit "deactivate". Check "opt out of future emails" to minimize your friends being able to tag you, send you messages, etc.
  - Deactivation leaves ghosts of you on facebook for your friends – you may still show up listed some places but shouldn't be publicly viewable while deactivated.
  - To fully delete an account, go to https://www.facebook.com/help/delete_account . Please note that "request deletion" in your regular settings does NOT delete your account – it's a preference for what happens in the event of your death.

- Make everything private. If there's no reason for anyone to see it, make it private to just you. If you want to share it with others, make sure it's friends-only, but limit this as much as possible to minimize damage from any slips. There's a lot of nitty-gritty iterations on facebook especially. For a walkthrough of some privacy settings to check and where, try this guide (but do your own checking as well) https://www.socialpilot.co/blog/ultimate-guide-manage-social-media-privacy-settings
- Change your name and your username if you have one. You may have a "username" that shows up as the url to access your page facebook.com/purpledinosaur would take you to Purple Dinosaur's page or anyone who claimed the username first. To change this, go to your general account settings and change both the name and the username at the same time. This will avoid your new name being found from the old url and your new url being found by your old name. Choose iterations of these that are hard to guess. NOTE: Facebook pages can

also be accessed by account id (assigned number different from username), so do not rely on this to provide full protection from tracking – if your adversary is clever, they may have saved the account id. If you need full disconnect from a past account's presence, start fresh with a new account.

- For public pages (businesses, band pages, personal accounts that are useful for organizing, etc.) consider carefully what goes up with an eye towards your community. You've chosen for this to be a public way you operate, have friends in pictures? Go through and remove information on and pictures of anyone who hasn't explicitly told you they're comfortable being public.
- Have someone with a burner account that's not attached to you go through and tell you what they can see. Have someone that's a friend-of-a-friend do the same. It's super easy for things to slip through the cracks.
- Unfortunately, getting rid of data on Facebook sucks. Like, really sucks. Here are a couple tools to try and make it less terrible.
  - Tagged photos are pretty much going to have to be done by hand. It's a slog. Set aside a good chunk of time or just do a little bit every day to be closer to where you want to be.

f/oallcdoceahndjmaalbicbcgpfnajgae?hl=en Congratulations! Now you can delete these things.

  - There are also extensions to delete "likes" and posts that can be used. This is going pretty deep but if you've ever liked a post on any sort of radical or leftist page, that stuff gets looked through ad can be a way to trace you. In the fall of 2017 there was a "doxx of all members of Antifa" that was really just a list of everyone who liked facebook pages with "antifa" in the name but it does tell you that adversaries understand that what you engage with is a good way to find you. Both of these are a bit of a slow process and can miss things, so you'll probably have to run it a couple times. However, there are options to delete within certain date ranges or from keywords if you don't want to get rid of everything.
    - Chrome extension: https://chrome.google.com/webstore/detail/fbook-post-manager/ljfidlkcmdmmibngdfikhffffdmphjae?hl=en-US
    - Firefox extension: https://greasyfork.org/en/scripts/9106-facebook-timeline-cleaner
  - To the best of our knowledge, you will have to remove group memberships and events manually. It sucks. It takes forever. It's also very worth it, especially if you've ever RSVPed to an event with public attendance or been a part of a facebook group that might be seen as targetable.
- Don't forget about your messages! Clean out inboxes, sent mails, and chats the same as you would for your email.

Follow this same approach for your instagram, twitter, etc. Be intentional about what can be seen.
