Preventing Non-Consensual Release of Personal Information

Securing your personal identity is always important. Being “doxed,” having your personal information as well as your banned political views broadcast to the world, can be a personal and professional disaster. A dox can handicap future opportunities both in and outside of activism.

Allowing yourself to be easily identified can tie you to other movement members and expose them to security risks, and place you at the center of blame for the actions of others. If nothing else, you should secure your identity to protect your brothers.

This guide is intended to help you avoid being a victim of doxing by opposition activists.

What follows are some basic tips to keep your identity as a political dissident unknown to your opposition.

Need to know...

- If somebody does not need to know information, do not give it to them.

- If you do not need information, don’t ask for nor accept it.

- Compartmentalize information about future operations — if somebody is not involved in the planning and execution, leave them out of the loop.

Your identity in activism...

- Do not use your real name. At a minimum, do not use your full name. Use your assigned alias whenever pertinent. Get used to using this functionally normal alias in person and online.

- Do not tie your real identity to either the movement, or other movement members’ real identities.

- If possible, do not use your phone. Use a burner phone. At a minimum, do not carry out organization-related communications over text messages or keep other members in your contact lists. Channels of communication moderated by the organization are more secure, but should always be treated as if they could be made public.

- Avoid using your residence for simple meetups with individuals who are not fully trusted. For simple pickups, instead find a neutral location nearby. If you must, understand that this ties your identity to the movement. Use good judgement on who you can trust.

- Understand that your license plate is linked to your name.

- If you must use your phone number to communicate with other members, although it is discouraged, be mindful of social media applications that “sync” your contacts and can give away accounts you previously thought to be secure. Notable examples: Instagram, Snapchat, Facebook, Twitter, Venmo.

Your online movement identity...

- Don't use variations of your name, or other personally identifying information in any usernames. Don't use your real email as any sign-up email. Avoid, if possible, as much personal information conveyed even in a personal email.

- Do not use the same usernames, profile photos, or bio information across platforms which could be used to search for personal details about you. Avoid posting the same content at the same time, even.

- Do not tie your activist online presence to your real online presence. This is a sure way to get doxed if someone is looking. Even something as simple as a "like" or repost links the two accounts, and could lead to a doxing.

- Little bits of information you give out can add up into a very complete picture of who you are. Remember that any piece of information can become a foothold to find others.

- Be wary of getting carried away in voice communications. Do not say anything that you would not have released to the public if the worst were to happen. Do not say anything so particular that it could lead to the release of your information.

Your "real" online identity...

- The best policy is to simply have no personal social media at all. Public facing social media is by far the most common way doxes occur.

- Information, personal or political, about you can also be stored or distributed by people you affiliate with. Be mindful of photos, information, or details about you that can be found on the profiles or pages of family, and friends.

- If you must have an online identity, stay on top of privacy settings. Lock it down to people who are not screened. Do not convey information to those you do not personally know.

- Do not tie your real online identity to other movement members' real online identities. This is a sure way to set up a situation where multiple people get "chain-doxed."

- It's a good practice to keep your "real" identity apolitical, even among friends and family.

- Do not publicly display your membership or affiliation with linkage of personal and non-personal social media accounts, or by having visible promotional material on your person such as stickers, patches, shirts, hats if it is not immediately necessary with activism.

- Do not have a voicemail attached to your cell number which includes personal details about you. This is a good way for people to verify your name with your number, and any other details which may be available to them.

- If you are deleting social media accounts, business profiles, or anything of the like, alter the details before deletion so that the account is as unrecognizable as possible and leave the account that way for around two weeks until it is deleted. This will update cached versions of the account to further protect your information.

Your identity during IRL actions...

- Properly plan actions so that you are not likely to run into trouble. Surveillance cameras, arrest records, police incident reports, vigilante camera crews, and media coverage can and have all lead to doxes.

- You should avoid public events which are not organized by the organization, but if you must attend one,

wear a mask if appropriate. Otherwise, wear large glasses, a ball cap and perhaps a hood or scarf depending on the weather. That disguise, while not perfect, is better than a full-on picture of an unprotected face.

- Do not wear clothing during actions which has any identifiable information on it such as your school, work, hometown, or anything else which can lead to the rest of your information.

- If you are at a masked public event, be aware that at some point you have to leave the event. Know how and when you plan to remove the mask and “blend back in”.

- Make sure all photos of you are combed through to have identifying features scrubbed before appearing in public channels of communication or social media. Tattoos, shirts with the logo of your school or place of employment, clues to where or when the photo was taken, recognizable scars or skin discolorations, any part of your face, neck, ears, or even hair.

- Avoid group photos. At the very least, have the photo circulate through as few people as possible, ideally one or less, before all identifying features of participants are obscured.

- Do not keep your supplies for activism easily found within your house or vehicle. If police were to search your home for an unrelated reason, make sure that they would not easily find stacks of posters, stickers, banners, etc.

- Again, be aware that your license plate is tied to your name.

Scrubbing the internet of clues...

The following websites assemble information on people, then sell it to the highest bidder. Most all of them have a way to remove the information by request. This information helps doxers to work their trade. Often, they have a tiny scrap of information to start with. Sites like these give them extra scraps, and pretty soon you are known. Go to these websites, and remove your personal information.

• Intelius.com

• Acxiom.com

• MyLife.com

• ZabaSearch.com

• Spoke.com

• BeenVerified.com

• PeekYou.com

• USSearch.com

• PeopleFinders.com

• PeopleLookup.com

• PeopleSmart.com

• PrivateEye.com

• WhitePages.com

• USA-People-Search.com

• Spokeo.com

• PublicRecordsNow.com

• DOBSearch.com

• Radaris.com

• https://www.instantcheckmate.com/opt-out/
• fastpeoplesearch.com

• peoplelooker.com

Further hardening your online identity...

- Use Tor, or a general VPN for online communications. Tor is a browser that routes communications through multiple nodes, obscuring the true identity of the user. Unfortunately, authorities examining your internet records will see that you use Tor, you can avoid this by using an alternative VPN. Likewise, if you sign into normie accounts with Tor, you are "burned" for that session in the browser.

- Turn off Bluetooth and Wifi unless they are in use.

- Do not use Google. - Close online accounts that you do not need. Photobucket, old blogs, forums, Github, and Amazon are all useful services that can leave little clues about you dangling. At a minimum, manage them.

- Understand that "smart" devices have a way of creating security breaches by storing reams of data about you that can sometimes be easily accessed by outsiders.

An example is a step counting app that puts you at the site of a major event, and publicly posts your exercise. You don't need the "likes." Turn this stuff off.

- University and genealogy websites may provide information about you against your wishes. - Take care when sending out movement-related documents that the document doesn't contain "meta-data" which will list you as the author. Particular culprits are Microsoft Word, and Google Drive.