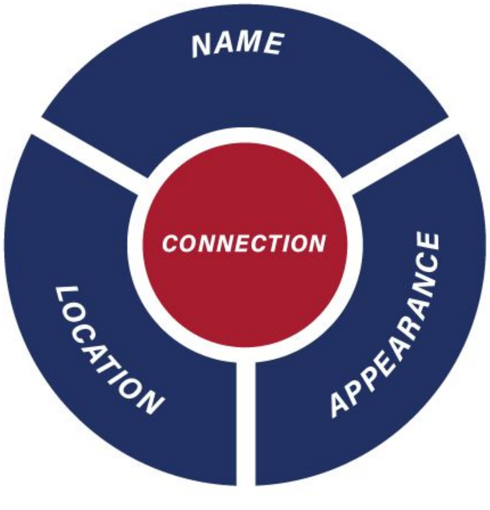
Preventing Release of Personal Information

As a member of an organization preaching opposition to the powerful, is vital to prevent any methods that said powers may use to silence you. Securing your personal information is the most important method to take in preventing much of these tactics of silencing dissent. They cannot harass, persecute, or assault anyone without first knowing who they are, or where to find them. **Your anonymity is your most valuable possession as an activist.** This cannot be understated. **Nearly every tactic of your opposition must first uncover your identity to implement their silencing tactics or harassment.**

Allowing yourself to be easily identified can tie you to other members and expose them to security risks, and place you at the center of blame for the actions of others. Securing your anonymity is synonymous with protecting the actions and safety of the organization as a whole. **Being careless in these matters represents a direct threat to the security of the organization, and as that is the case, it is non-optional to abide by the following guides.**

Nearly every release of personal information follows a similar structure.



In order to complete a “dox”, your opposition will need three primary items, with a fourth secondary item, to fully compromise one’s information. Without any singular piece of the whole, the collection of information is not complete. Your goal, in defending against these tactics of intimidation, is to prevent your opposition from getting any piece of the whole, and at the very least, connecting all four.

Your real name should be withheld in all cases, your specific location of residence should be restricted, and your appearance should be guarded, all in line to keep your enemies from establishing a final connection with the organization. **It is vital to compartmentalize these aspects of information from each other, as well as making as many of them as completely inaccessible as possible.**

It should be noted that while those initially uncovering information may seem relatively powerless and easy to perceive as a mere annoyance, the very same information will then be carried up to much more powerful members of the opposition. A release of information can start with isolated social media insults, and scale into full scale legal and political harassment by law enforcement with unwarranted searches, and the removal of basic constitutional rights, even without any crime being committed. **This can all be avoided with very simple and practical levels of caution.**

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 in any context unless it is absolutely necessary. If you are in a situation with another member in which they must use their real name, excuse yourself if you are available. Use your assigned alias in every pertinent circumstance. Get used to using this functionally normal alias in person and online.

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

- Do not use your phone number or texts for organizational matters. Use a burner phone if you must use standard phone calls. 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 and thus interacted with along proper lines of caution.

- 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 organization. Use good judgement on who you can trust. When in doubt, don't.

- Understand that your license plate can be linked to your name and other information by law enforcement or other determined individuals. Use rental vehicles in circumstances where it is not feasible to hide the license plate of a vehicle during an action.

- 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 activist identity...

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

- 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. Randomize usernames, profile images, and account styles that you may use online.

- 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. It is not worth the risk in any instance.

- 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.” Do not ask for or share these accounts with others.

- It’s a good practice to keep your “real” identity apolitical, even among friends and family. Do not share internal information about the organization to even like minded friends or family. Keep your membership secret to as many people as possible.

- 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...

- All actions must be properly planned with all security precautions in mind. Surveillance cameras, arrest records, police incident reports, vigilante camera crews, and media coverage can and have all lead to doxes.

- Public political events which are not organized by the organization should be avoided, 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. Even in these instances, leadership should be consulted.

- Remember that, as a member, everything you do has the potential to represent the organization. Do not carry out any actions which would place the organization or its members at risk if your membership were to be publicly disclosed.

- 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. Even commonly worn clothing, or clothing that appears on personal social media posts should be avoided.

- 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, recognizable scars or skin discolorations, any part of your face, neck, ears, or hair.

- Avoid group photos. At the very least, have the photo circulated through as few people as possible, ideally one or less, before all identifying features of participants are obscured. Tattoos should be covered in all instances where they may be seen. They can be blurred or obscured in photos, but the spot on the body where the tattoo is often still visible and can still potentially identify an activist.

- 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.

Meeting intermediaries...

- Meet in a public space. Ideally a space with several buildings and walkways nearby.

- Arrive 15 to 30 minutes early. Drive or walk around the general area to look for any people walking around who may look out of place. Keep an eye out for groups. If you are doing activism later during the meeting, scout the route that you are planning to take so you know the area.

- Do not park immediately within view. If possible park at a nearby establishment to the one you are meeting the person at. Try to avoid being seen getting out of or into your car by the applicant.

- Ask the intermediary to convey what he will be wearing. Examples are what color of shirt, style of jacket, type of hat or sunglasses. This way you can see him before he sees you.

- Ask the intermediary to stand, sit, or be generally around a local landmark like the front of a store, foundain, bench, statue, or street corner. Do not be immediately at this location.

- Once you have visual confirmation of the intermediary from a distance, send the specific shop, address, or area you are at to him or make your approach.

- Ask him to keep his phone face up on the table, and depending on your level of concern, ask the intermediary to close any open applications he has on his phone or turn the device off entirely.

- Look for items that could hide cameras on his person. Pens in front pockets, water bottles, or any devices clipped to his clothing.

- Topics to talk about should be primarily dependent upon the intermediary's responses in the interview stage of the evaluation process, but valuable points of reference should be his personal political history, and his aspirations with the organization. You should be keeping a mental list of key points in the conversation.

- Doing some light activism in the form of stickering or placing other materials are suggested, and you should be mindful of the mannerisms of the intermediary. Don't let him run off on his own or get behind you for long periods of time.

- Some coaching on the best way to take photos of the placed material should also be done in this case, and is a good opportunity to look for notifications on the top of his device which may indicate a recording application being open or anything else suspicious.

- Make sure you are not seen getting back into your car by the intermediary. Don't give a for sure message on their membership status until you have fully concluded the meeting and reported back to leadership with your findings.

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.

- 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.