A GUIDE TO DATA PROTECTION FOR PROTEST AND REBELLION.

I'm not a data privacy professional, but I've tried my best to make a guide that helps beginners in the world of data protection easily keep their data private and help protect others in the process as well. If you have any questions DM me at Owl#5806 on Discord and I'd be glad to help

PLEASE DO NOT READ ONLY THE SHORT VERSION, IT SHOULD ONLY ACT AS A REMINDER FOR YOU LATER ON.

THE SHORT VERSION:

VPNs – Only use a trusted VPN, enable Kill Switch and Auto-Connect on all devices, if you can't afford to pay for one, I suggest using ProtonVPN

Browsers - For daily use, use Firefox, for more suspicious activity use TOR

Search Engines – Don't use google, use DuckDuckGo for regular use

Mobile Device Usage – DON'T bring your phone to protest, if you need comms, safely buy a burner phone and never have it on (including battery) outside of the action zone. Watch for stingray towers and use encrypted messaging services like Signal. NEVER EVER record video or take photos of people's faces at protest, it can end very badly. If you aren't doing too many suspicious things, make sure to signal jam and confuse and overwhelm government systems, like enabling and disabling location and mobile data services at random intervals

VPNs:

VPNs are incredibly useful tools in keeping your information safe, but there are things to keep in mind when using them.

1: They CAN and HAVE been breached, always keep an eye on breaches from the VPN service you are using. Do keep in mind that VPNs are still very important if you can afford them Even when they are breached it is incredibly difficult for the hacker to get to specific information, especially if the website you are visiting uses the HTTPS communication protocol, you can check this by looking for https in the address bar or clicking the lock icon on the menu of your browser.

2: Free VPNs can be a bad idea. Usually they target the market of people who want to access region-locked content and who care much less about privacy. Most free VPN or proxy services still farm your information and sell it to advertisers. The main free VPN that *does* keep your data safe I've come across is ProtonVPN, they do keep your data encrypted and private. They do have downsides that they note while comparing the free vs paid versions on their site. It also doesn't require a credit card which may be useful to some of you. ProtonVPN: [https://protonvpn.com/]

3: Considering recent events and repealings (Patriot Act) of yet more online privacy protection rulings, you should go into your VPN's settings, enable Kill Switch and Auto-Connect. This means that if your computer disconnects from the VPN you can't accidentally send out unencrypted information, and when you boot up your device or otherwise disconnect from the VPN it will automatically reconnect you.

4: It is a good idea to get a paid VPN if you can afford one, look for online deals from places like your favorite YouTube channel, this supports the creator and often the savings on offer can be surprisingly good.

5: I won't recommend specific VPNs -there are many- but I implore you to do thorough research on it before buying. I personally use NordVPN, I used a 70% off deal for their three year plan. They have had a data breach in the past, and have spoken about their increased standards and fixed practices. They are one of the leaders in the VPN industry, and I do trust them to provide private access. It's your call if you agree with me, but the good thing is that there are plenty of other services to choose from.

6: Even if you use a VPN, if you use services that collect data through interactions anyways the VPN will NOT protect you. For example, if you live in California and use a VPN for Alaska, but continue to buy packages for your home address in California, then the services you use will clearly know where you are regardless of where the signal is coming from. This is why the below information is also very important to stay safe online, and to keep the extra information collected on you to a minimum. VPNs won't help you if you continue to use the same accounts, or use a phone number somewhere on a website maybe to log in. MANY things can be used to track you, but if you want privacy specifically when looking into protest a VPN is a very important tool. For full privacy, that can take a lot more effort to make sure that services don't know anything about you, like using aliases, middle man phone numbers like VOIP, and fake intermediary credit cards, among many other things.

Browsers:
Browsers are important tools, and the way they treat privacy is incredibly important. Chrome is a browser produced by Google which has been consistently criticized for allowing trackers liberally and pushing users to continue to use the google ecosystem. I suggest Firefox as an alternative, it's run by a nonprofit company focused very openly on privacy, it has many more dedicated and visible controls for trackers, search history, and account safety. Mozilla (Firefox Devs) also has a dedicated extension for Facebook services to keep them contained to their own tab (which can also be used to access multiple email services and accounts the same window, like a personal account signed into YouTube and a work account signed into Google Classroom on the same window which can be useful for keeping certain accounts clean of information). Another browser for maximum security would be the TOR browser, TOR is a dedicated service specifically made to keep data private from governments, it is often sent to countries under oppressive governments to help rebellion. I would recommend using TOR more for illicit or suspicious activity than day-to-day use, as it is slower than most browsers. That is because it (in the most basic terms) sends the information out to many other computers also using TOR to confuse signals and make everything impossible to trace. This also means that the more people using TOR the more effective it becomes. It is often cited as a good browser to access the dark web, but as a simple search machine it works quite well too. TOR can be a good option if you can't use a VPN, and many VPNs also support using TOR/Onion (TOR = The Onion Router) Servers instead of one of their own. TOR Browser: [https://www.torproject.org/] NOTE FOR MOBILE: There are multiple versions of Firefox available, I use Firefox Preview, anything from Mozilla that is a mobile Firefox browser should be good. For Android users, there IS a mobile version of the TOR browser, unfortunately there ISN'T an official one on IOS, there are TOR browsers, but not by the TOR Project themselves. They have endorsed THIS TOR browser, so I suggest you use it too: [https://apps.apple.com/us/app/onion-browser-secure-anonymous-web-with-tor/id519296448]

Search Engines:
Search engines are the thing you use to actually find information on the internet, and can be used to track you very easily if you aren't careful. First off, DON'T USE GOOGLE. Just don't. They are constantly following you every move and click and are a massive corporation not to be trusted. This is a link to the page of data Google has tracked from you, for those of you who have been using google unprotected it can be enlightening, especially how long the list is:
[https://myactivity.google.com/myactivity?hl=en&utm_source=google-account&utm_medium=web].
I highly recommend switching to DuckDuckGo a service specifically designed for privacy. Although the switch might seem painful at first, it's surprisingly easy and very important to protect your information, they don't require you to make any kind of account and never store your data, the search experience is still quite good.

Mobile Device Usage:
Here are a few tips to keep in mind when using your mobile device for protest purposes.
1: DISABLE ALL LOCATION SERVICES. Cops can EASILY track you and your location history. I'll get further into why this is kind of moot when it comes to actual protest but this is just a good rule of thumb if you're not willing/able to do any other stuff. Just have them off at all times unless you NEED to use a maps app, though again only do this if you aren't willing to signal jam and mess with data.
2: DONT HAVE YOUR PHONES ON AT PROTESTS/DONT BRING THEM TO PROTEST AT ALL as you can see in this post, [https://void-slvt.tumblr.com/post/619473543889125376/leave-your-phone-at-home-period-if-you] even with location services disabled, cops can still track you through Stingray, which fakes a cell tower and tricks your phone into giving data about it's location and ID. Even a VPN wouldn't be able to help you because Stingray doesn't use the actual data sent, but instead triangulates you position which can be done even with a VPN on. Again, as noted in the post, if you need to contact someone else at a protest, buy a burner phone with cash somewhere that is safe to shop at (make sure that the shop doesn't use too many trackers and identifying services that could help cops ID you) and never have the battery in and the burner phone turned on outside of the protest area. Otherwise, simply don't bring your phone to the action zone. A useful site to see the status of Stingray use in your state: [https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them]
IF YOU ABSOLUTELY MUST BRING YOUR PHONE TO PROTEST: Take your phone to the action zone TURNED OFF, only turn it on if you NEED the communication, always have the VPN on (as it does still help mask your data) and use an ENCRYPTED messaging service, a good one would be Signal: [https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en] / [https://apps.apple.com/us/app/signal-private-messenger/id874139669] and also install an IMSI (Stingray) tracker/warning app. SnoopSnitch and Android IMSI-Catcher Detector are both for android, they don't prevent the connection or data transfer, but do warn you when you connect to a Stingray tower. SnoopSnitch: [https://play.google.com/store/apps/details?id=de.srlabs.snoopsnitch&hl=en]
Android IMSI-Catcher: [https://cellularprivacy.github.io/Android-IMSI-Catcher-Detector/]
3: MESS WITH DATA PATTERNS
[https://hater-of-terfs.tumblr.com/post/616405431691231232/queeranarchism-afraidofamericans] Do this especially if you aren't doing anything suspicious, so if you're someone who isn't able to attend protests and wants to help DO THIS. Enable and disable location and data services at random intervals, USE apps to confuse and complicate the data signals being received by the government and companies. (NOTE: Please check the post, I didn't make this list, this is taken from the post and user hater-of-terfs on Tumblr)
Ad Nauseum [https://addons.mozilla.org/en-US/firefox/addon/adnauseam/] is an adblocker that stores the ads it blocks and continuously generates fake clicks, fucking with analytics and costing the ad companies money
TrackMeNot [https://addons.mozilla.org/en-US/firefox/addon/trackmenot/] automatically does randomly generated searches on a variety of search engines to obscure your real searches and fuck with analytics, and you can set it up to work with anything that has a search bar (including facebook, twitter, amazon, youtube, etc)

WhatCampaign [https://addons.mozilla.org/en-US/firefox/addon/whatcampaign/] replaces analytics parameters in links with the string "FuckOff". I thought there was a similar extension that used random strings, but I can't seem to find it

Privacy Possum [https://addons.mozilla.org/en-US/firefox/addon/privacy-possum/] is a fork of Privacy Badger with a focus on costing tracking companies as much money as possible, and idk if my

limited tech knowledge is enough to understand what it does but the description does say it falsifies some data so that's good enough for me

4: DON'T RECORD OR TAKE PICTURES OF PEOPLE AT PROTEST. This is a big issue, it massively compromises the safety of anyone you record. If you feel truly compelled to take photos or videos DO NOT share them online. Again if you feel compelled to ignore this warning, the absolute baseline to follow is to carefully censor any and all faces of protesters in the video or photos, otherwise you could be responsible for the safety of another person being compromised, they could be arrested, attacked, or even die.

Sources:

https://privacysos.org/blog/how-to-defeat-fbi-or-police-stingray-surveillance/

https://www.pcmag.com/opinions/after-a-breach-should-you-still-trust-your-vpn

https://www.vox.com/recode/2020/5/13/21257481/wyden-freedom-patriot-act-amendment-mcconnell

https://www.cnet.com/how-to/what-is-tor-a-beginners-guide-to-using-the-private-browser/

https://youtu.be/CNRdHQJ9AMk

https://www.nbcnews.com/news/us-news/ferguson-protester-edward-crawford-subject-iconic-photo-found-dead-n755401

https://blog.torproject.org/tor-heart-onion-browser-and-more-ios-tor