PROTECT YOURSELF

a primer on digital and physical resistance

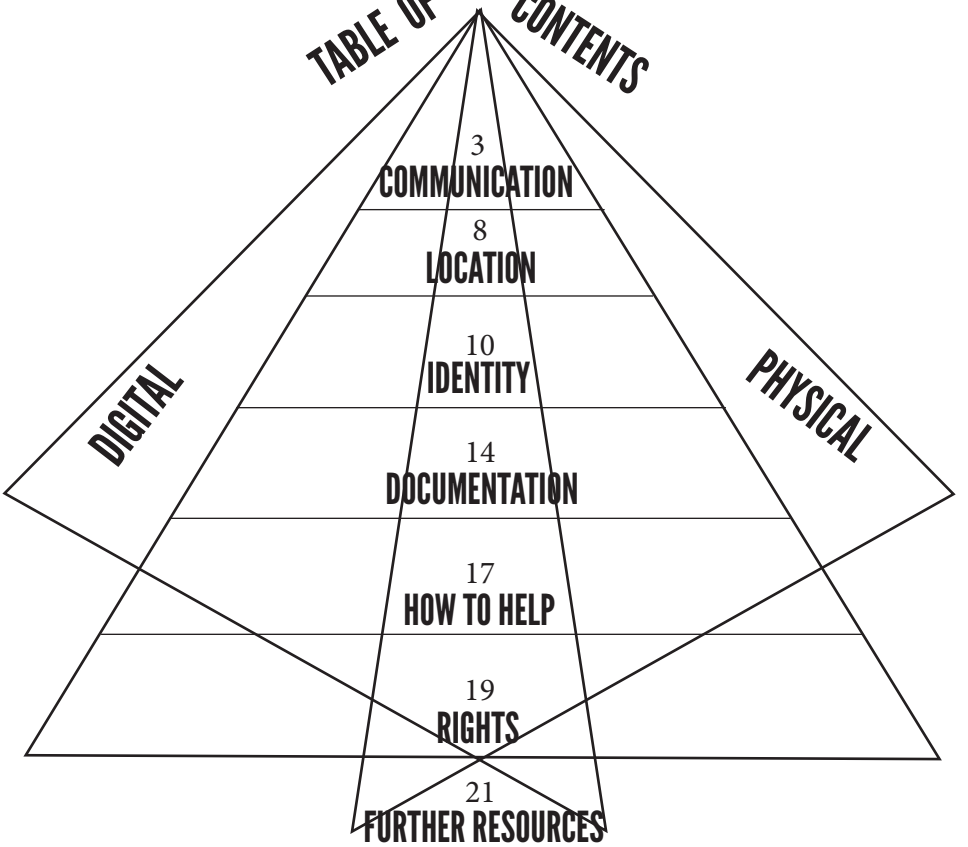
Resistance in Digital and Physical Spaces?

Why present digital and physical methods of resistance together? This question grounds the argument that this zine attempts to make through the information that it provides. This zine hopes to highlight the importance of identifying the ways surveillance is enacted by external forces that leverage the junction points of where the digital meets the physical. When your digital presence becomes physical and vice versa, traces exist that make it easier for you to be surveilled, tracked, and recorded. Suggestions on how to protect yourself against surveillance in the digital and physical worlds will overlap quite a bit; that is to say separating the digital from the physical in terms of surveillance techniques and protections is becoming an increasingly difficult task.

Even one's digital presence is physical. Computers store information on hard drives; the internet relies on modems, routers, and physical wiring to function. The physical is also digital, one can be tracked in physical space through digital means, such as by your cell phone's GPS, rideshare usage, or through the data that your phone or applications collect. Therefore, when using different methods to resist surveillance, the digital and physical cannot be thought of as separate entities. Both need to be taken into consideration at the same time, otherwise new possibilities for surveillance are created. The connection between digital and physical surveillance is important to take into account not only so you can protect your privacy, but also because the information gathered through the means listed below can be used to detain and prosecute you.

This guide is not meant to be a comprehensive list, but a starting point for activists and others interested in securing and protecting their online and physical presence. We have worked hard to make this guide easy to read, understand, and implement. That said, no method is completely secured from eavesdroppers; meaning that even the best methods of hiding one's online and physical self are subject to survaillance. Additionally, improperly implemented security methods can put users at greater risk, so we recommend if you choose to adopt any of our suggestions, conduct additional research on the topic to see what others in the security and activist community are suggesting, as technology and tools are constantly changing and new vulnerabilities, even within highly regarded security methods, are constantly being identified.

TABLE OF CONTENTS



Communication

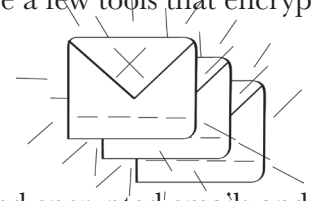
Digital communication happens through a number of devices, from smartphones to video game systems. There are so many digital technologies that allow us to connect with others, making it challenging for anyone to keep track of what or whom is communicating in any instance of use. Connected to these complex digital communications are he ways we communicate in the physical world blend into the digital realm. Communication technologies encompass phone calls, text messages, emails, SnapChat, Instagram, Facebook, and any other way people share information with others. Digital communication does not just include the devices we own, but also the applications we run and use. Each one of these technologies can be used at home or out in the world, which creates a complex web that can be used to keep us under surveillance.

Technologies such as the telephone have been used for communicating with others for decades. They ways that governmental institutions, such as the police, could monitor telephone use was straightforward: the police could request a wiretap and listen in and record phone calls. Now, with the popularity of smartphones the police and other governmental entities can do much more than just record your telephone calls. By using a digital communication technologies (think a computer or smartphone) authorities can monitor, record, and store every bit of information transmitted through your device: all of your text messages, phone calls, Facebook conversations, emails, etc. Even with your device turned off and password protected your information is still at risk of being recorded. Again, this is not an exhaustive list, but a starting point to better understanding the connections between digital privacy and the physical world.

Digital Protection

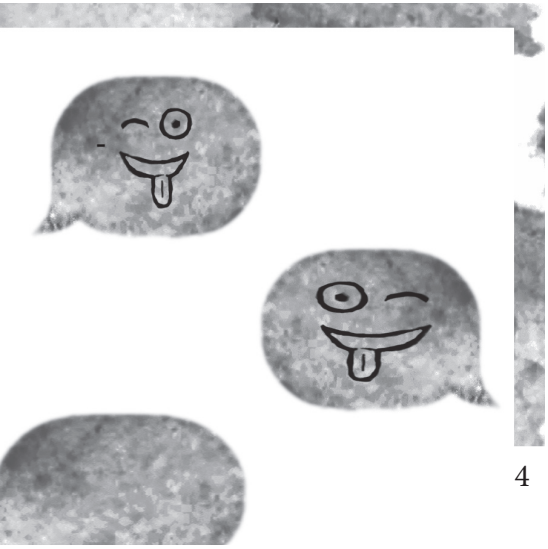
Besides turning off your devices (including removing the battery – which is impossible with Apple devices) there are ways of hiding your communication from those who would like to like to surveille and record it. The main way that you can protect your communication information is through encryption.

Encryption scrambles your information for everyone *except* those who key to unscramble it. Imagine you are sending an encrypted text message to a friend, they need a key to unlock the text message, without the key the text message looks like gibberish. This process can be complicated, but there are many free services that greatly simplify the process! Below are a few tools that encrypt different types of digital communication:



Email

Proton Mail (https://protonmail.com/)
This is a free service that allows you to send encrypted emails and attachmentss to other Proton users. You can also send encrypted emails to non-Proton email addresses, but you will need to provide the receiver with a password to unlock the email (this is the key!). This software is free with some limitations on how many emails can be sent per day. This service works on any computer, and has applications for the iPhone and Android devices.



Text Messaging

Signal
https://whispersystems.org/
A free application for both the iPhone and Android devices. Signal allows for encrypted text messaging between phones with Signal installed.

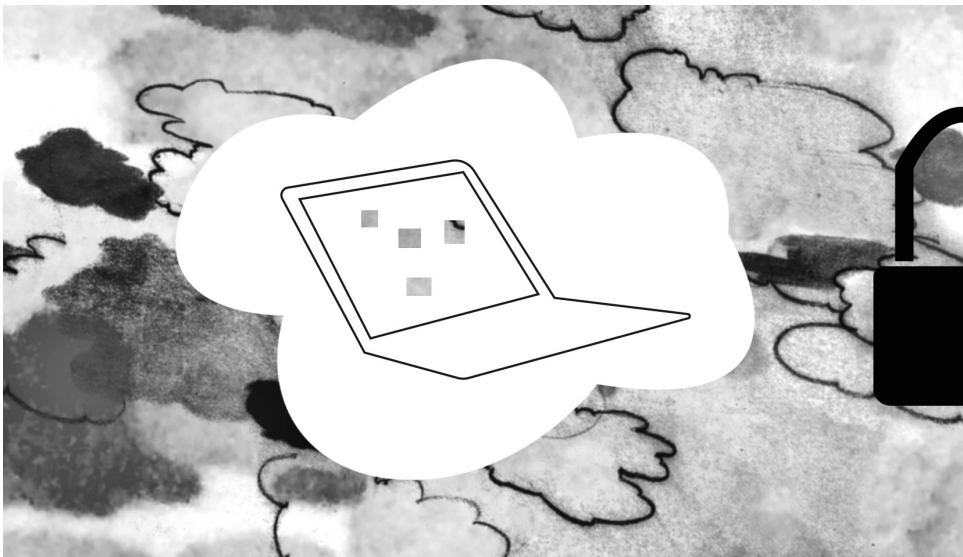
General Internet Usage

AirVPN (https://airvpn.org/) AirVPN is a virtual private network (VPN) service that allows for any internet usage to be encrypted, and allows the user to make their internet connection appear as if is coming from different parts of the world. This is achieved by having computers all over the world that subscribers can connect to as a means to connect to the internet (this service costs about $40 a year. There are free services, but their encryption methods and data collection are problematic).

Hard Drive Encryption:

Windows: **BitLocker** - This comes with Windows 7 and beyond. It is suggested you research this independently before using. If you do choose to use this, it is very simple to setup.

Mac: **FileVault** - This come with the Mac OS. In settings -> Security & Privacy -> FireVault once this is turned on your hard drive is encrypted. Again, we strongly suggest doing additional research before encrypting your entire hard drive.



File Encryption

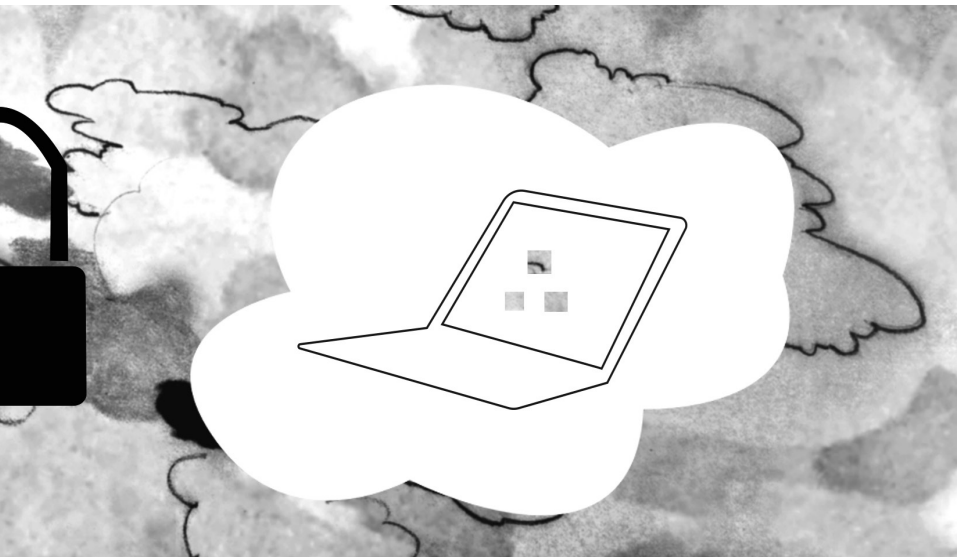
Encrypto: (http://macpaw.com/encrypto) This software allows the user to drap and drop single files into the software and become encrpted. The files can be unlocked via a user generated password. The software is free and works on Windows and Macs.

Cloud Store Encryption

BoxCryptor (https://www.boxcryptor.com/en): This sofrware works with Google Drive, DropBox, and Box and allows the user to encryt their files within the cloud. The software is free for personal use.

Physical Protection

Popular surveillance practices often target both the digital and physical realms. By working to break this link, it will further protect your communications. Physical communication tracking can take place through many methods such as through cell phone spoofing (where police and governmental agencies create fake cell phone towers to collect and track information communicated over cellular networks) to intercepting your text messages in real-time. These are just two examples of how your physical communications can be tracked.



How to avoid having your communication surveilled and tracked in the physical world

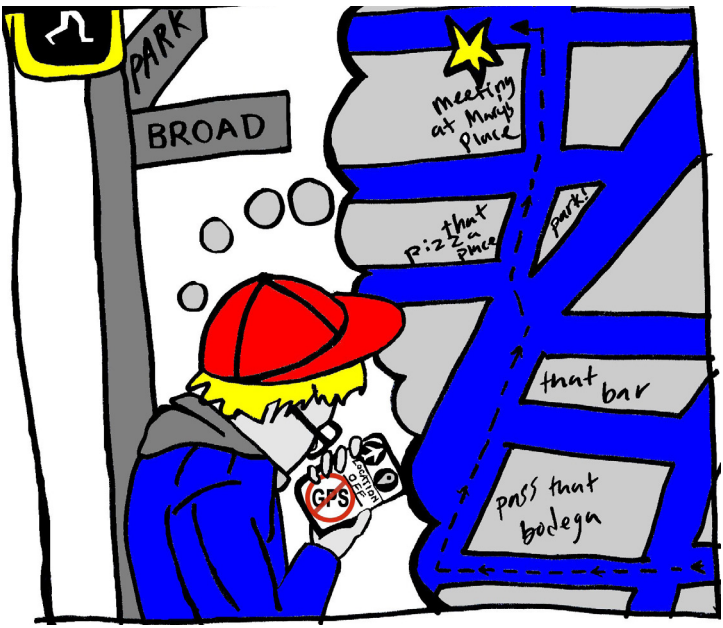
1. Leave your smartphone/cellphone home and have predetermined (through encrypted means) meeting spots.

2. Use walkie talkies over encrypted channels (special walkie talkies are needed for this).

3. Turn off everything except BlueTooth on your phone and use point-to-point communication hardware to chat and share your location with others.

- **GoTenna** (http://www.gotenna.com/) is a point-to-point communication hardware that works with iPhones and Andoird via a BlueTooth connection and encrypts your communication.With this device no cellular network is needed.

4. Do not share your intended final destination online before leaving.



Location

A person's location can be easily be tracked through many means, including through your smartphone or your home computer. This is accomplished through either global positioning satellite (GPS) data from your smartphone, a cell phone's cellular connection, a computer's IP (internet protocol) address, or by physically following you. Think of an IP address like your home's address.

The groups that can surveille a person's location through GPS or other means are government entities, generally speaking, from the local to the federal level as one's location can be collected from anywhere. With location data, institutions can easily determine where you are in real-time, but also know where you have been, for how long, who you are with (by collecting other's location data), and can determine what activities you are taking part in. This information can be used to prosecute and identify you, and/or use the location information to identify others you have been in contact with. Overall, location data can be use to make many assumptions about the person being surveilled.

Digital Protection

The suggestions on how to avoid having your location tracked are similar to those to avoid having your communication surveilled:

1. Turn off your cell phone, or better yet, leave it home.

2. If you must use your phone, use a VPN to hide your location, and if you are using a smartphone (please refer to the communication section for additional VPN information), but you must turn off cell phone connectivity (i.e. airplane mode) and use Wi-Fi.

3. Do not post your location publicly online.

4. Turn off location features on all smartphone applications, and/or turn of location tracking all together via your phone's settings.

5. Turn off location awareness on your social media applications.

Physical Protection

With your location information, surveillance and governmental institutions can use this information to prosecute and detain you by linking your movements to actions or events that may have taken place in the area you were. Additionally, they can use your location data to link you to others people an agency is surveilling, thus expanding their knowledge of how you organize, meet, and who the members are.

How to avoid it

1. DO NOT take Uber or Lyft to get around. Take public transportation (using cash), walk, or better yet, ride a bike!

2. Don't use Google Maps or other online mapping tools as these services create digital trails ahead of your physical movements, and mark your destination.

3. Mix up your daily routines, making it harder to know how, where, and when you are traveling.

4. Use cash and not credit cards. Credit cards digitally transmit your information when paying for a service, which includes the point of sale location.

Identity

Your online identity is you; it is a digital representation of yourself. You should protect your identity online as if it is your physical identity. Both your physical and digital identities are tied together in many ways. Your online identity is a combination of pieces from different parts of the internet: your social media presence, your email address (including your contacts, the emails you send, and the emails you receive), what search engines you use (i.e. Google), along with how and what you browse, and the cookies - small files created by websites stored on your computer that contain your web browsing information - you generate. This is in no way a complete list of the ways online identity is created, but highlights how your online identity is compiled and how your digital identity is connected to your physical self.

Your physical presence can also be photographed, video recorded, and audio recordings can be used as methods to identify you. With photos and video, governmental agencies can use facial recognition software to determine who you are (your driver license photo is usually what governmental agencies use to match a photo of a person to a name and other identifying information).

Digital Protection

The implications of having your digital, or online, identity monitored or even stolen are great as online identities have great value.The value can be monetary, social, or have value in the information that an identity contains. When different entities want to track and identify a person digitally, there are many methods to do so, which were discussed in previous paragraphs. With the identification of your online identity, governmental agencies that wish to track you have many tools and methods that can be used to follow the tracked person from their home (internet use while at home) to anywhere else the tracked go through using the information your smartphone generates, facial identification, and

traditional tracking (i.e. following you on foot) once you have been identified. With this said an online identity holds value as it can be the foundation to tracking all of your movements, communication, what you buy, and any other digital and physical movements or transactions you make. This information can be used to detain and prosecute you! Your digital footprint ***IS*** you!

How to avoid it

We suggest ***not*** using social media to communicate and organize. While we know these platforms are how the majority of people communicate and connect, they are also highly monitored Social media is not only public, but the companies that own them can also be compelled to release private communication because the communication is in plain text (not encrypted).

If social media must be used, have multiple accounts that are not linked directly to your personal profile and that are ONLY used for activist communications. Additionally, when using your secondary social media profile, use a private browser tab (FireFox and Chrome both have this feature). All this does is separate your browsers from your previous cookies. Also, connect to a VPN to hide where you are connecting from and to encrypt your online usage.

1. When signing up for new services, you do not need to be truthful-- use false information to make the account harder to trace back to you.

2. Connect to a VPN before conducting any online communications. VPNs are discussed in detail in the Communication section of this guide.

3. Put tape over your webcam. There is evidence that suggests governmental and other entities surveile users through webcams.

4. Watch for emails that are phishing for your information. The form many phishing attacks take is posing as a real online service you subscribe to, and asking you to reset your password through a link. It is always better to navigate to the website in question, independent from the email link, and see if your password or other information actually needs to be reset.

5. Generally speaking, break up the services you subscribe to: don't use Google for everything, don't use Facebook for all of your communications. Break up how you choose to represent yourself online which will make it harder to put the pieces together for those that are tracking you.

Physical Protection

The information that is collected in the physical world is then used as information to link you to your digital identity, location, and communication. The implications for this are great, as once your physical identity is know it will be easier for entities to track your digital presence, and vice versa.

How to avoid it

1. Use bandanas or masks that cover up portions of your face There are makeup and hairstyles that make it harder for facial recognition software to function. A good example of this is CV Dazzle (https://cvdazzle.com)

2. Use infrared emitting lights that show up on many cameras as a bright white light (http://tinyurl.com/irglassesir)

3. Clothing that reflects light, making it difficult to take photos of your face. An example of this is the Flashback collection (https://www.betabrand.com/collections/flashback-reflective-clothing.html)

4. Do not drive your car if you do not need to. Licence plates can be automatically identified and tracked.

Documentation

The documents that are records of one's identity (e.g. birth certificates, marriage certificates, citizenship papers), actions (e.g. police reports, court transcripts, news articles), status (e.g. resumes, degrees, titles, employment contracts, tax forms), and other important aspects of life (including religious documents or cultural documents) are vital to ensuring the integrity of each human being's experience and can have serious consequences for the person involved if altered, lost, stolen, or made inaccessible/overly accessible. These records could exist in several media, most commonly as both physical or digital documents, or as either physical or digital only. Because in the last two or three decades many records that existed previously only as physical documents have now been digitized or are digital-born (originate as digital), several of the ways they are managed (or even thought of) have yet to catch up with these new forms. This section looks at some examples of how both types of documents (physical and digital) function in current society and suggests some ways you can make sure they function to your benefit.

Physical Protection

Since physical documents may only exist as a singular material object, they could be destroyed without a trace if not protected. Physical documents are vulnerable to damage from natural disasters or otherwise, theft (including being photographed or removed from trash), and being misplaced or lost. In addition to protecting a physical document, securing digital copies of important documents is a way to keep them organized and accessible; however, once digitized, several versions of that document then exist and it becomes more difficult to monitor and secure all copies. For instance, when using a document management system or cloud-based file sharing program, understanding who has access to that content and to what extent is

vitally important, especially if the documents contain sensitive or identifying information.

While some records are visible (like most physical documents), some digital records are produced implicitly as part of larger systems online that track user activity and may exist as several copies in different locations. Websites make use of web cookies to remember your login information, previous searches, recent activity, etc. Most of these companies sell or share your information to third parties, such as data brokers, who collect information about individuals and sell it to other companies or the government.

Certain laws and policies, like Computer Fraud and Abuse Act (CFAA) [http://tinyurl.com/c83ocn8] of 1986 that regulates authorized use of the Internet, or the Patriot Act (2001) [http://tinyurl.com/mqeuckq], which along with Rule 41 [http://tinyurl.com/zapcbte], can allow for warrantless searches and over-broad data collection by the governement, contribute to the necessity of awareness of one's digital records and traces. With all of these collection activities, it is difficult to know what information has been collected about you, where it will end up, and what the potential is for prosecution.

On the other hand, records and collected information could also be used to resist oppressive activities. Unfortunately, hate crimes have been occurring more frequently since the outcome of the 2016 election [http://tinyurl.com/zwtp892]. One important and effective way to combat this hate is to produce a record of witness of these crimes so that they do not go unnoticed, with victims silenced. Recent efforts to collect and document hate crimes have appeared and should be utilized, including Southern Poverty Law Center's (SPLC) harassment reporting site.

How to avoid it

1. Make paper copies of documents that are important to you and keep them in a safe location (like a disaster-resistant safe or vault).

2. Also make digital scans/copies of important documents and save locally on your personal computer or hard drive to use as backups.

3. Make sure they are organized and easily accessed if/when needed.
4. Shred all documents with identifying information before placing in the trash.

5. Be careful to never misplace an important document as they are vulnerable to theft or damage (for instance, do not leave in printer tray, visible on car seat, or some place a easily seen, damaged, or taken).

Digital Protection

1. Clear your Cookies from each of your browsers periodically (usually found in History settings) or set your browser to "Private" or "Incognito" mode so that cookies will not be collected.

2. Always use a VPN when connecting online, and especially when using a computer with public internet service (Wi-fi).

3. Change passwords and security question answers often. Choose passwords that are long and contain numbers, letters, and special characters. Use a password generator rather than your browser's web cookie system to keep track of your login credentials. Password generators can flag you if you have weak passwords and can safely manage and sync several browsers with this information for a small cost. Highly rated password software includes LastPass [http://tinyurl.com/jzvaen4] and Dashlane [http://tinyurl.com/zwdozdy].

4. Keep track of the commonly visited websites' data policies with this browser add-on that rates Terms of Service agreements: [https://tosdr.org]

5. Do not sign any paper documents without reading them first

and asking for a copy (you still have a right to possess a copy of any physical document you sign)

Creating records of witness:
• ACLU Recording Application: [http://tinyurl.com/jy5vhxs]
• Southern Poverty Law Center's (SPLC) harassment reporting site: [http://tinyurl.com/ztv2yoe]

Take care when filling out any documents with your identifying information and ask yourself the following questions:
• Who will now have this information? Do I trust this person/entity with my information?
• Is it possible that this information could be passed on to any other entities? (third party, like the government, marketing firm, or data broker)
• Do not sign any paper documents without reading them first and asking for a copy (you still have a right to possess a copy of any physical document you sign)

How to Help

Several physical and digital locations that facilitate connections with people, entities, and resources can serve as places of information, even respite, for those affected by changing policies and government structures. Often, it is simply a matter of locating these locations and resources and reaching out, whether as someone who can utilize their services or someone willing to donate time to help others in need. These locations (whether physical or digital) are usually publically-funded and can help you find information about protecting yourself, finding aid, or just provide a safe space when you need it.

When peoples' rights are violated, often they feel overwhelmed and do not know what steps to take. This can lead to a population of people who feel disenfranchised from the government or

community, powerless to remedy their situation, and do not make use of the resources available to them. With so much information being spread around at a rapid pace online, figuring out physical realities (such as which campuses or cities have designated themselves "sanctuaries" and what exactly does this mean) can be difficult to determine. Moreover, when discussions both online and in-person have become increasingly heated and divisive, a simple action such as asking for help can seem more intimidating than necessary.

One thing to think about is how your activities are being tracked – a common theme throughout this zine. As you seek help, remember to take precautions when searching for resources both physically and online that could incriminate you or someone else involved.

Physical Protection

1. Make use of public resources.
Most locations that receive public funding (state-funded institutions, universities, libraries, clinics) can offer information, resources, and/or aid to their communities. This might include medical or legal help and information finding assistance. Show up in-person, ask for help or to be directed to other sources of help, and make use of all information. Often locations may hold events that are open to the public (speakers or talks, medical aid, fairs, etc.) where one can gather lots of information quickly and ask questions to real individuals. Be sure to take all necessary precautions to protect yourself and others when reaching out physically and digitally.

2. Find safe locations.
Since the election, many places have offered their advice and space to persons feeling threatened by the possible policies of the incoming administration. Several cities and college campuses have designated themselves 'sanctuaries' for undocumented citizens, for instance, protecting their privacy and not cooperating with

the authorities. Public libraries also have extensive experience and training helping people find resources, can often offer a sympathetic ear, and also generally respect their patrons' privacy. Even if you are not enrolled as a student or member, these locations may serve starting points for information or even spaces to talk or rest.

Digital Protection

1. List of sanctuary campuses: [http://tinyurl.com/hbu69jb] (might be out of date, check each university's website to see up-to-date information)

2. List of sanctuary cities: [http://tinyurl.com/ndpjwz7] (this is an ongoing issue, make sure to double check all information)

Rights

Ideally, a democratic society ensures the justice and equality of all citizens rather than upholding the will of just a few; with this in mind, America's founding statements (Declaration of Independence and the U.S. Constitution) include stated rights and protections provided for the people living in this country. Additionally, with the Internet providing another hopefully democratic space, expected affordances by its early users were stated in various manifestos and analyses of this technology--an extreme example of which is John Perry Barlow's 'Cyberspace Independence Declaration' that describes the (hopeful) ability of cyberspace to liberate users from their physical bodies and material consequences. While this declaration is important to think about, especially with concepts such as 'Net Neutrality' [http://tinyurl.com/gp9ghkg] being threatened, where the FCC classified the Internet as a public utility with the intent to ensure more equitable access to all, whether cyberspace is completely unregulated or regulated to ensure equality, the physical and material realities for

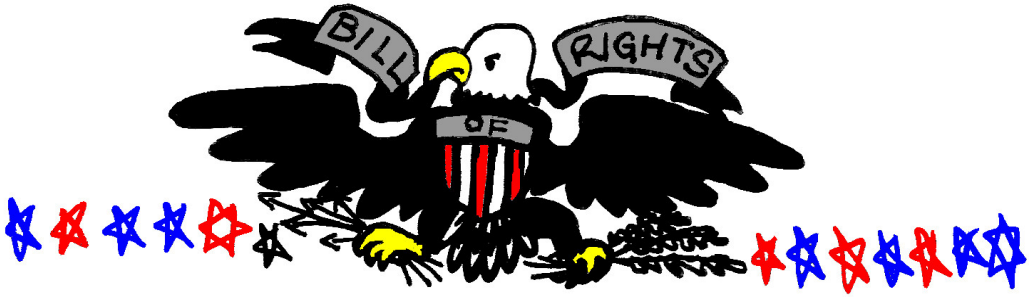
users cannot be separated from this digital space.

Although it may sometimes feel that these rights are a given or guaranteed in some way, in practice, these rights are frequently violated and ignored by governmental agencies, and further disenfranchise and marginalize people of color, women, members of the LGBT community and more. In truth, these rights are only 'guaranteed' by certain mechanisms, like laws and their interpretations and enforcement. For instance, understandings of 'privacy' may vary in the way our 'right to protection from unreasonable search and seizure' (Bill of Rights, 4th Amendment) is maintained--does this right ensure privacy that means a certain amount of anonymity or total anonymity? What types of actions/identities/affiliations/activities do you think should change this definition?

Therefore it is important to remember that the interpretations of these rights can change based on a handful of people's opinions and values (politicians, courts, judges, regulatory agencies, and legislative bodies), meaning their very definitions and outcomes for citizens can also change. Learn, know, memorize and, most importantly, always keep at the forefront of your mind these statements which guarantee you certain affordances:

We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are ***Life, Liberty and the pursuit of Happiness****.*

July 4, 1776
Declaration of Independence



Freedom of speech, press, religion and petition.

Right to keep and bear arms.

Protection from quartering of soldiers.

Protection from unreasonable search and seizure.

Right to due process of the law.

Right to trial by jury, speedy trial, public trial, counsel.

Right to civil trial by jury.

Prohibition of excessive bail and cruel and unusual punishment.

Protection of rights not enumerated in the Constitution.

Protection of the powers of the states and the people.

Amendment 14: Citizenship rights – This amendment, ratified in 1868, gives the right to citizenship to anyone born in the U.S. It also gives citizens the right to equal protection of the national and state laws, the right to be free of any law that deprives a person of life, liberty or property without due process.

Amendments 15: Voting rights – This amendment, ratified in 1870, gave people the right to vote, regardless of race or color.

Amendment 19: Women's voting rights – This amendment, ratified in 1920, gave all citizens the right to vote, regardless of sex.

Amendment 26: Voting age – This amendment, ratified in 1971, gave all citizens age 18 or older the right to vote.

Source: http://www.americansentinel.edu/blog/2011/09/07/how-the-constitution-protects-our-rights/

Further Resources

- EFF Surveillance Self-Defense: https://ssd.eff.org/en
- ACLU Technology and Privacy: https://www.aclu.org/issues/privacy-technology
- Violet Blue's Smart Girl's Guide to Privacy: [http://tinyurl.com/z9yjbk9]
- Oh Crap! What now? Survival Guide: [http://tinyurl.com/jasmzec]
- http://assets.lapdonline.org/assets/pdf/demonstration.pdf
- https://www.amnestyusa.org/pdfs/SafeyDuringProtest_F.pdf

Information Rights Research Group, 2017
Illustrators: S. Apostolides & Sophie White