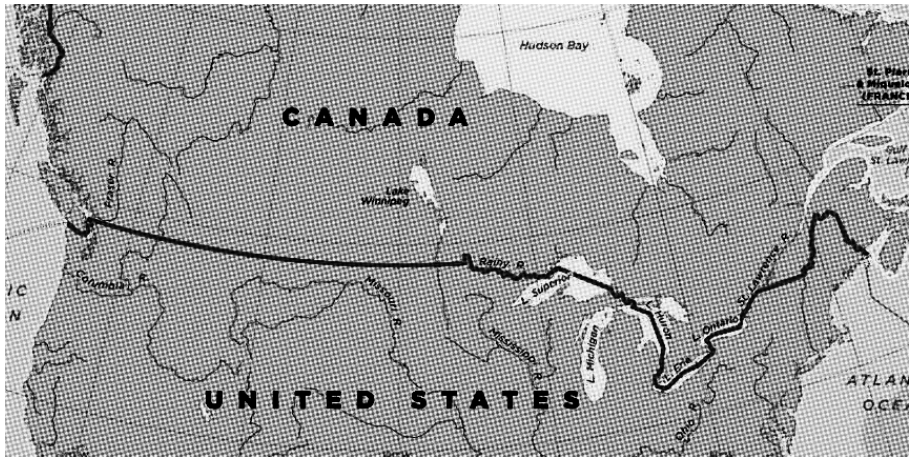
The information contained in this zine is meant for people trying to cross at legitimate border crossings. We are proposing a standard of practice where we do not "inform" on our friends and community when crossing the border. […] [W]e hope to inspire conversations on "best practices at the border," so that we can keep each other, and our networks, safer.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.

Crossing the U.S./Canada Border

A Proposal for Best Practices



Crossing the U.S./Canada Border: A Proposal for Best Practices

Original text in English

Crossing International Borders: A Proposal for Best Practices

2019

New edition

No Trace Project

2023

Layout

No Trace Project

notrace.how/resources/#crossing-u-s-canada

Resources

- Digital Privacy at the U.S. Border: Protecting the Data On Your Devices[11]
- Know Your Rights: U.S. Airports and Ports of Entry[12]
- No Wall They Can Build[13], a Crimethinc book and podcast series
- Undoing Border Imperialism[14], a book by Harsha Walia
- Electronic Devices Privacy Handbook: A Guide to Your Rights at the Border[15] by the British Columbia Civil Liberties Association
- Border Security: Canada's Front Line, a reality TV show about the CBSA

[11] https://www.eff.org/wp/digital-privacy-us-border-2017

[12] https://www.aclunc.org/our-work/know-your-rights/know-your-rights-us-airports-and-ports-entry

[13] https://crimethinc.com/podcast/no-wall-they-can-build-1

[14] https://www.akpress.org/undoing-border-imperialism.html

[15] https://bccla.org/our_work/electronic-devices-privacy-handbook-a-guide-to-your-rights-at-the-border

all the answers to these questions, and surely the answers are constantly changing.

It is more than just individual choices and judgements that make up our collective strength. We've already seen how our isolated "choices" in dealing with the border have negatively influenced our relationships and networks. We recognize an urgent need to fortify our security culture in this area. Let's create a cultural practice to deal with the border so we can take collective responsibility for our safety.

Contents

Introduction

You drive up to the U.S. border in your car. The border guard asks you where you live, where you're going, how long you'll be staying, the purpose of your trip, and then out of nowhere says, "pull over here, leave your phone in the car, and come inside." A tight knot in your belly forms as you realize you didn't prepare for this moment. You thought that having an honest story and wearing a nice shirt would be enough. You try to remember if your phone is encrypted and you realize it's not. Uh oh.

As anarchists, we know not to give the police information about our friends if we are arrested or questioned. It's standard practice security culture. However, many anarchists cross international borders regularly and interact with border guards. Border guards are agents of the State and should be considered as much of a threat as the police. By crossing border checkpoints, we volunteer ourselves to be questioned and possibly further investigated. As anarchists actively engaged in struggle, we believe that it is important to keep as much information about our networks as opaque as possible. The more they know about us, the more they can, and will, use it to further repress our movements and struggles.

Borders are becoming more militarized and outwardly racist. New laws and executive orders have come into place that give border guards increased powers to detain, refuse, as well as increased access to the information shared between countries. Nobody is an exception. They target everyone so as to build intelligence and better control movement of people. As their capacity to gather information grows, so too do the troves of data in our phones, social media, and electronic devices. We need to ask ourselves serious questions, like:

- What can we do and say so that we don't accidentally give up information about our communities/friends at the border?
- When does your desire to cross the border become not worth the risk to your community?
- What are your "rights" at the border?

Conclusion

Always be fully prepared to go through border checkpoints, a lot of that involves planning ahead and getting consent from people you might have to admit to knowing. We feel it is worth re-stating that at the border you should never answer any questions about anyone else—even if it seems benign—without their complete and full prior consent. And you should never unlock your phone (unless it is a burner phone without any friends contacts or social media connected to it). Otherwise, your phone MUST be encrypted and turned off.

Before you go, update yourself on your "rights" at the border. Investigate how your digital information, social media, and web presence can be used against you and others. Have a plan for what you will and won't say, practice it, and decide beforehand how you will handle the problem of phones. Memorize a lawyer's phone number.

You must be prepared to not get in not informing on our friends/networks is more important than crossing the border.

The recommendations made in this zine are based on the idea that the strength of our networks and movements is compromised when the State knows more about us. The more they know, the more able they are to repress us.

There is a lot we still don't know about crossing borders safely. What is the amount of communication between border guards in different countries? Do they keep track of what you tell them each time? How do you know if you're on a terrorist/no-fly list[9]? What are the consequences for refusing interrogations, fingerprints or retina scanning? What are the legal consequences of being caught lying at the border? Every border will be slightly different, but they all serve to collect information and to control the movement of people. We don't know

[9]The 2019 version of the no-fly list of the Transportation Security Administration—the U.S. agency with authority over the security of transportation systems—has been leaked and is available here[10].

[10]https://sizeof.cat/post/tsa-nofly-list-download

A story

What follows is a story from an anarchist who weighed the pros and cons and attempted to cross the border:

> "I knew a lot of people who I had crossed with were being denied entry. I wanted to cross, so I contacted them and we talked about the pros and cons of my trying to cross. From other friends' experiences, I understood that were I to deny that I knew the people who I had already crossed with, I would likely be denied entry or banned. I also knew that when my name was Googled, an article about a public arrest and the names of my co-accused came up. I contacted all the people who I was certain the border guards would know about: people I had already crossed with before as well as people whose names appear next to mine as co-accused in a press article. We made a collective plan, synched up our stories, and agreed upon what information was okay to give to the border guards. Here are the questions we collectively decided to answer:
>
> - How did we know each other? (music scene, school, etc.)
> - Are we still in contact?
>
> I made a plan for how to cross, and practiced my answers with friends. I brought documents showing that I was in school, had a job, had a booking for a hostel to stay at when I crossed, and had plans to return to my country of residence. I decided to attempt to cross. As soon as my passport was scanned, even before they questioned me about my trip, an orange paper was printed out and I was brought in for secondary questioning. Here, they asked me about my friends I had already crossed with, and I gave the answers that we had collectively agreed upon. They asked me if I had ever been arrested before. They asked me about the people whose names appeared next to mine as co-accused in the media article. They asked me if I was associated with many different names, some of which I recognized, others which I didn't. I only gave them the answers my friends and I agreed upon, and no additional information. I was let through. I tried crossing not long after that experience. After a much shorter period of questioning I was denied. When I asked why I was being denied, the border guard threatened to ban me. I have not attempted to cross since this experience."

- How much information do border guards have access to?
- What information can they get from your phone?
- What kinds of questions are the border guards likely to ask?
- What kinds of behavioral standards should we hold each other to when interacting with border guards?
- What is considered solid and not solid practices at the border?

We focus here on the U.S./Canada border because it is the one we have the most experience with and the border that many of our comrades cross most frequently. We are hearing more and more stories about people being denied and banned at this border, and we have seen the ways that people being linked through intelligence gathering and border crossings has led to this current cascade of border repression. We know that the more information they get about our networks, the more that they turn people away.

The information contained in this zine is meant for people trying to cross at legitimate border crossings. We are proposing a standard of practice where we do not "inform" on our friends and community when crossing the border. We also realize that our practices need to continuously evolve under the rapidly changing technological and political contexts we inhabit. As society moves towards more surveillance technology and decreased privacy, the border has access to rapidly increasing levels of control over our bodies and social networks. There will come a day when we can no longer cross the border without compromising other people, so we should start thinking about creating other alternatives to official crossings. In the meantime, we hope to inspire conversations on "best practices at the border," so that we can keep each other, and our networks, safer.

Context

What do we know?

"Everytime, be ready to be denied."

Everyone must go through primary inspection, which is the initial questioning booth. Secondary inspection is when you are transferred into another space to be searched or questioned further. If you are pulled into secondary, you could be flagged or it could be random. If you go into secondary, you could still get in, it doesn't automatically mean you'll be denied.

Apparently if you decide to "withdraw" your request to enter the United States, U.S. border guards can still question you (specifically your reason for withdrawal), demand identification, search you and your belongings, and possibly even detain personal effects (like keep your phone).

We have comrades who have been denied entry to the U.S. and told to try again another time, as well as those who've been informed they are permanently banned from entering the U.S. We know folks who have been given time-specific bans (e.g. a five-year ban) as well as folks who have been turned away at one crossing, who then successfully crossed a few months later at a different crossing. We've heard of people who received a time-specific ban, fought it in court, and won. We also know comrades who are on no-fly lists, like Tuscan. Tuscan is a Canada/U.S. joint no-fly list with over 680.000 names—40% of which have "no recognized terrorist group affiliation"[1]. There is no known way to be removed from this list.

Through the United States Visitor and Immigrant Status Indicator Technology (commonly referred to as US-VISIT), a Customs and Border Protection (CBS) management system, the U.S. collects biometric data (such as fingerprints). This data is checked against a

[1] https://www.theguardian.com/world/2018/jun/30/canada-us-tuscan-database-no-fly-list-trudeau

- Your phone is now compromised. There are too many things that could possibly have been done to it, including installed intelligence gathering hardware/software, which makes the phone too dangerous to keep using afterwards. You must now get a new phone.
- If you didn't have it encrypted and off, you must also now consider everything on your phone to be compromised, including social media, all of your contacts, call history, bank accounts, etc. This is bad.

After attempting to cross

- You either made it or you didn't - either way your integrity is intact. Good job!
- If you were taken into secondary, as soon as you can, write down an account of what happened. What your story was, what questions they asked, your answers, etc. By comparing questions they asked, we can begin to create a map of the information they know.

If you fuck up at the border

A lot of the information put together in this zine is gathered from times we have fucked up. Let's try to avoid it. If it does happen—say your unencrypted phone is taken or you let slip who you're going to visit, it becomes incredibly important to:

- Immediately let folks who have been compromised know.
- Immediately make all the Signal groups that could have been compromised defunct.
- Get a new phone.
- Not get defensive or make excuses—you fucked up.

other email providers will absolutely hand over your information if the State asks for it.

- Set up a new email. Email providers that do not keep login information (such as riseup.net) will draw unwanted attention, so this new email should be from a corporate service like Gmail. It should be set up and accessed exclusively through your border phone.
- You could say you don't use social media because of all of the illegal information sharing.

How to look legitimate

- It helps to have some layers to back up your story.
- Print out plane tickets, concert/event tickets or listings, hostel/hotel info.
- Learn about cancellation policies so that you may actually buy tickets to events and/or hotels if need be, and be reimbursed later.
- Bring bank account statements to prove you have money to spend.
- Bring a pay stub and/or a lease to prove that you have responsibilities at home and you're not trying to immigrate into the country.
- If you have a minor, non-disqualifying issue on your arrest record, ask a lawyer for an undated but signed letter stating that the charges have been dropped, discharged, etc. This will be helpful if your record comes up. You can also get this from the court where your charges were passed through. You can ask the court for a record of your charges and their outcome.
- Declare something at the border. Get a bottle of wine or something from duty free, or declare your food. “Oh I have this chocolate bar do I have to declare it?”, “I do have some carrots and trail mix, is that OK?” or declare a gift for your grandma.

If they took your phone and give it back

database to track individuals deemed by the United States to be terrorists, criminals, and illegal immigrants. Canada also uses biometrics, specifically iris identification, through the NEXUS program, a joint program of the U.S. Customs and Border Protection and the Canada Border Services Agency (CBSA).

It's also important to think about how changing political contexts create problems for particular groups. For example, permanent residents. Under Canada's bill C-23, CBSA agents posted in U.S. airports and abroad can deny permanent residents from boarding their flight back into Canada if they feel like the resident has violated the terms of their residency. Permanent residents could then drive to a land border, however, if this happens overseas. However, as one CBC article[2] points out, if someone got denied at an overseas airport, they won't be able to make it to a land crossing and they could find themselves in the same straits as some U.S. green card holders in the first days of President Donald Trump's travel ban. Other sources suggest that if you're trying to get back into Canada, it's best to cross at a land border where both permanent residents and citizens have the right of entry. However, anecdotal evidence from friends suggests that, so far, they've received fewer problems taking flights versus land borders.

Your rights at the border

The border is a liminal space. Guaranteed entry into a country where you don't have citizenship isn't a right, so any choice you make might get you denied entry. For example, you can refuse to answer questions or give biometrics but you will likely get denied. Border interrogations take advantage of this. They have a rare opportunity to examine you without charging you with a crime. This is not generally legal or possible in many other situations. In the current context of international State collaborations, it is not unlikely that U.S. border agents could be doing interrogations on behalf of Canada or vice versa.

[2] https://www.cbc.ca/news/politics/pre-clearance-border-canada-us-1.3976123

It is important to research your rights at the border before you go as they may have changed recently. In researching this zine, the information on what rights you do or don't have varied depending on the source, so we can't vouch for it. It contradicts itself and just isn't clear. Therefore we'll keep it short.

When entering the U.S. or Canada, if you get detained during secondary questioning (if you are unsure, ask, "Have I been detained?") you can be searched and interrogated without a warrant. Never rely on border guards to give you accurate legal advice. Do no sign any papers without speaking to a laywer. You have no right to privacy, all of your electronic devices that you have with you can be searched, copied and potentially seized.

We couldn't find consistent facts on how long they can hold you if you've been detained (though some sources said 48 hours is the maximum going into Canada and 72 is the maximum going into the U.S.), or where you will be held during that time (if they will move you to an immigration detention facility while they wait to put you in front of a judge).

In both Canada and the U.S. citizens and permanent residents have a right to enter their country. They also have a right to speak to a laywer if they have been detained. Non-residents however, have very limited rights. It is unclear even if you have the right to an attorney (although you should absolutely demand one).

There are differing levels of privilege and risk while trying to cross a border. White supremacy and racial profiling affect who gets pulled in for questioning and eventually denied entry. People are routinely targeted because of their race or religion. Citizenship creates a two-tiered system where certain people have the "right" to enter a territory while others do not. One source ominously said the U.S. reserves the right to detain terrorism suspects "indefinitely"[3]. The State disappears people, to black sites like Guantanamo Bay and others around the globe. It is important to note that your "rights" can be ignored and revoked by the State, though it is also important to remember that due to widespread anti-Blackness and Islamophobia,

[3]https://www.immigroup.com/news/know-your-rights-canada-us-border

- "It's a work phone, unlocking it would violate confidentiality agreements"
- "I don't know the password" (you could have someone else reset the passwords before you leave and then get the passwords after you cross)
- "No. I'd rather not."

If you're asked why you don't have a phone or have a new phone

- "Oh, haha, I'm just unplugging for the weekend ;)"
- "I just broke/lost my phone this week, so this one is new/couldn't get a new one yet."
- "I left it at home because I didn't want to get charged for the roaming fees"

Set up a "clean" email, social media

- It's considered unusual to not have an email or social media. For this reason some people may choose to set up "clean" accounts to curate an identity that is not tied to their politics or anything sketchy.
- If you do set up a "clean" social media account, make sure you don't connect with anybody that you actually know. All in all, this is a questionable practice, as you could actually be potentially putting strangers at risk who are connected to your fake social media. It's a gamble. We don't know if there is a way to do social media without giving information about other people.
- Be careful not to give them things you use(d) in real life. To be honest, your Gmail address is probably sketchy as fuck, there are all kinds of wingnut emails you may have forgotten about which you don't want to give to the border. It might still contain your banking history, your music and podcast choices, search history, online purchases, and friend contacts. Gmail and most

someone is flagged or banned, this could give everyone they've crossed with border problems too.

- If you do cross with your friends, when they ask how you know each other you could say it's a rideshare or you're carpooling to a concert—the less tight your relationship seems, the better. Then, in the future if you're asked you can stick to that story.
- If you are asked about someone who you've crossed with before multiple times in the past, it doesn't make sense to deny knowing them. What are some options of how you can respond? The music scene is a good place to meet and travel with people who you don't know very well. You crossed together to go to shows multiple times because you're into the same type of music. The most important is to NOT give any more information about that person to the border.

When you are asked about people by name

When you are asked about people by name, or if things get intense in the interrogation, here are some things you could say:

- "I don't remember" and "Not that I recall" are potentially good ways to not give up information and not to be straight up lying.
- "I have never heard that name before"
- "Would this be a good time for me to call my lawyer?"
- "Am I being detained? Can I call my lawyer?"
- "This is getting intense, I think I should talk to my lawyer"

Also:

- Make sure you have or have memorized a lawyer's number.
- Remember, the only exception (to giving more information) is if you have an agreed upon story with someone about how you know them.

When asked to unlock your phone

the people most likely to be affected by these scary outcomes are brown, Black, and Muslim people.

Basically, what we know is that you can be detained without a warrant, get searched (both externally as in a strip-searched or internally as in "bedpan vigils"—where they put you in a cell without running water until you defecate and then inspect your feces). You can have your property confiscated/destroyed, your electronics taken and the information on them copied. You can be fingerprinted and have your retina scanned, and potentially be interrogated for days. Interacting with the border isn't something anarchists should take lightly.

Secondary inspection

If you get pulled into secondary, the first guard will keep your passport and bring it inside and hand it over to the person who will question you. You'll go inside, there's often a waiting area, you'll wait until they call your name. You will eventually get called up to be questioned by an agent. Sometimes you can end up getting pulled into a more enclosed area for further questioning. Sometimes they search your car.

Being targeted for secondary inspection can be random. It can be based on a guard's suspicions or prejudices, based on a flag on your file that comes up when the guard scans your passport, or based on your travel history. It can also come from information received from the Interagency Border Inspection System (IBIS). Customs and Border Patrol (CBP) officers rely on this system to determine which individuals to target for secondary examination upon arrival in the United States. CBP, along with law enforcement and regulatory personnel from 20 other federal agencies or bureaus, use IBIS. Agents can access the IBIS system using a network with more than 24.000 IBIS terminals, located at ports of entry including border checkpoints, seaports, and airports.

Remember, there are things that can get you flagged which are not necessarily related to being an anarchist: sex work, drugs, working

at a weed shop, and/or DUIs[4] (Canada automatically refuses people for DUIs, the U.S. automatically refuses people suspected to use/sell any drugs including cannabis).

If you're pulled into secondary inspection, it could be because they want to search your car, to ask more information about your travel plans/proof of work, to look for proof of your "story" in your phone, or to question you as part of an ongoing investigation. Secondary inspection doesn't necessarily mean you're flagged or will be denied. However, if they start asking into your interests, your networks, your technology, your deeper history, or especially when they start asking about other people, this is when it may be difficult for you to continue trying to cross without informing on your networks.

The next few sections of this zine are to help prepare you for getting through secondary inspection without informing on your friends and networks.

[4]Driving under the influence (DUI) is the offense of driving a vehicle while impaired by alcohol or drugs.

Strategies

Have a clear story. Know exactly what you can and can't say.

Your travel plans

- Explore your non-political interests. When asked your reason for crossing, here are some ideas for reasons: concert or music related, a festival, university related event, tourist attractions and/or events, etc.
- Print out the information for the event you plan to attend.
- You could buy a ticket to an event and have it printed off.
- Research the place you say you're going to so that you can talk more confidently about what your intentions are there.

Your relationships

- If you have a sympathetic family member on the other side of the border, it can be very helpful to use them as your reason for crossing. (Note: people's family members have been visited by the FBI in seemingly border-related investigations, so this strategy will not work for everyone.)
- If you're dating someone on the other side of the border, it's usually a bad idea to tell the border as they might believe you're trying to immigrate. That being said, if you are trying to immigrate, it might work in your favour to be forthcoming with the dating information—in this case you should talk to an immigration consultant and consider their advice.
- If you ever cross in a car with someone, you will forever be associated with them. Consider that this might be a good time to stop crossing with your friends. Crossing together allows them to build information about our networks, and in the future, if

- Factory resetting your phone: If the device was not encrypted before the factory reset, then it is possible old data may be recovered afterwards. Border guards can see that a factory reset has been done recently and this has been a basis for suspicion in the past.
- Deleting apps: This doesn't work. If they have access to the phone's storage, they can recover deleted app data. This kind of data recovery is done on a routine basis.
- Deleting sensitive messages, contacts, etc: This is the worst thing you can do! If they get access to the storage, the first thing they do is a forensic recovery of the deleted data, giving them an immediate summary of all the information you didn't want them to see.

In short, your options are:

1. Don't bring a phone. However that could raise suspicions.
2. Encrypt and turn off your regular phone, and be prepared to refuse to unlock it, and for them to potentially confiscate it.
3. Have a burner phone that doesn't have your friend's contacts or your social media accounts on it.

Best practices for border crossing

> "You may not think of yourself as the threat they are looking for, but you don't know what information they can glean from your information and social networks. They ask so many kinds of questions that all contribute to a broader picture. Every time you cross you might be helping them."

Our ideal standard would be to not give border guards any new information at all. So, what might they know already? Different levels of border guards know different amounts of information. The first border guard at the primary inspection booth has much less access to information than the guards do in the secondary inspection area. In the secondary inspection area, the guards are more likely (though not guaranteed) to know: who you've crossed with, your border crossing history, who you've been arrested with, who you're publicly associated with, and your criminal history. They are NOT likely to know anything about your tax history, employment, bank accounts, health history, or your address.

What is considered not solid?

Here is a list of reasons that people have given for why they feel it is OK that people share information about other people at the border. They are excuses we need to move away from:

- "There wasn't any repression because of it." (which meant, "no one ended up in jail because people talked")
- "That person is just bad at getting interrogated and that's OK. People are good at different things and it's OK to be bad at getting interrogated." (if you think you're gonna be bad at getting interrogated, maybe don't cross the border)
- "We really wanted to get in and otherwise wouldn't have gotten in."
- "Everybody talks at the border."

- "No one told us that there were community norms about not talking at the border. We didn't know people were having problems, no one shared strategies with us about what to do."

Here are the absolutely NOT solid practices:

- Answering any questions about anyone else, even if it seems benign, without their complete and full prior consent.
- Not encrypting your phone or having it turned on or unlocking it at the border (unless it is a burner phone without any friends' contacts or social media connected to it).

The following sections give more details and ideas about how to cross the border in a SOLID way.

Preparation

Consider the fact that you might be interrogated. This can be a consequence of being a part of a political community/communities that hates the State. Prepare for the fact that you might not get in. It's more important to keep our networks safer than it is to cross the border.

Decide on your overall strategy based on your reason for crossing and consider different travel methods. How badly do you need to get across? Is your grandma dying? Do you want to go to an anarchist event or see friends? If you absolutely need to cross, is there a way for you to cross that will make it less likely that you will get questioned? Can you cross with your parents or other blood family? Can you fly across, drive a car that is newer or a rental?

In preparation, long before you get to the border, check your luggage and your whole car for pamphlets, newspapers, zines, stickers, receipts, business cards, mail, and anything else political. Make sure you don't have anything with anybody else's name/address/phone number on it. Also do a drug sweep for joints, drugs, pills and alcohol. This includes drug residue, so clean any card which was potentially used to crush drugs, like credit or ID cards. If you're bringing any harm reduction materials like condoms or safer drug use material, this could also be used against you if searched.

If you have an expensive phone, you might want to consider not bringing it across the border. We know that people are more likely to unlock their phones under pressure if it is expensive/difficult to replace.

If you want to avoid being placed in the position of having to refuse access to your device (and consequences that go with this), then don't bring it with you.

If this is your situation, here are some options for what you can do instead:

- Bring a special "border phone" that you have not used at all, or that you have very intentionally used only for a limited set of things that you have evaluated as being less sensitive to border surveillance. Be sure to check with anyone who is connected to this phone (through contact list, call history, etc.) before you take it across. Also, something that may seem very normal to you may still be an issue at the border. For example, be careful about not having political music or podcasts on your burner phone. The intentionally-used version is less likely to be suspicious to border guards, but it is risky because phones can record more information about yourself and others than you realize. Only do this if you're somewhat confident about how phone metadata works. If you can't afford a used border phone, you could instead collectively buy a shared border phone that is factory reset between users and only has limited contacts of family or people whom support your crossing story, a clean search history, etc. This phone would have to be changed if ever closely inspected because the phone's hardware serial number would link together the different people collectively using it for border crossings.
- Buy a phone on the other side of the border that you switch to when you get there.
- If you don't cross with a phone, work on preparing a plausible reason why this is the case, as having no phone has been considered suspicious at the border.

Things that may not work as well as you would hope:

It is important to choose a strong password that won't be easy to be crack. The No Trace Project recommends either:

- A password made of seven random words created using the Diceware[5] method. Such a password can be generated using the KeePassXC[6] software or with physical dice[7].
- If your phone limits password length too much—which should not be the case if you follow the No Trace Project's recommendations[8] on mobile operating systems— you can also use a password made of 16 completely random lower-case and upper-case letters, but such passwords are typically harder to memorize.

Finally, this may seem obvious, but still needs to be said: despite all the possible consequences, you must not unlock your device at the border, nor share your password with the border guards! Not complying with their requests for access to your device means they can detain you for many hours and confiscate your device for months, if not indefinitely. They will claim that their experts will be able to break into your device anyways so you might as well just give them access, however, if the device is encrypted with a strong password and turned off, this is likely not true (we know the cops lie to us, no surprise the border guards do too). If you don't have citizenship, they can, and likely will, deny you entry if you do not comply. If you're bringing your device to the border, you have to be prepared to accept these consequences, They will try to use these consequences to coerce you into turning over our shared information and that is why we have to prepare in advance to defend ourselves.

In addition, if the border guards take your phone out of your sight and give it back to you, you must consider it compromised—get a new phone. Things could have been done to its hardware or software that allow it to be used for further surveillance once it is turned back on.

[5] https://en.wikipedia.org/wiki/Diceware
[6] https://keepassxc.org
[7] https://www.eff.org/dice
[8] https://notrace.how/threat-library/mitigations/digital-best-practices.html

- Anything that you need or want on the other side, you can mail to yourself instead of taking it with you.
- Before you cross, check in with people you've crossed with in the past and agree on whether you can say you know them, how you say you know them, etc.
- Use the "Questioning" section below to practice your answers to the questions they will likely ask, including when you stop talking.
- Use the list of options at the end of the "Phones & electronic devices" section below to decide ahead of time what your electronics' strategy will be.

We think that it is NOT SOLID to cross the border without making these preparations.

Questioning

As mentioned previously, it is standard practice security culture in anarchist circles to refuse all questioning when you are arrested by police; you only have to give your name, address and birthday, and ask to talk to your lawyer. By contrast, it's not exactly reasonable when crossing a border to refuse all questioning. It will basically guarantee that you will be denied, maybe even banned from that country, and it could cause problems for other people you've crossed with. So how do you know when to stop talking? How do you know when the risk of informing on your friends/comrades becomes not worth crossing the border?

We know that border agents start with superficial, or more innocuous questions in order to build up to bigger ones. Try acting out the following lists of questions with a friend. Actually practice speaking your answers, so that at the border it will feel more natural and you will be more confident. Decide beforehand what is your bottom line for what you will answer.

They almost always ask: What is your citizenship? Where do you live? Where are you going? How long are you staying? How do you know the other people you're traveling with (if you're in a car to-

gether)? What is the purpose of your visit? Do you have anything to declare? Where do you work? Do you have any cannabis products? Do you have any weapons or firearms?

They sometimes ask: Where are you staying on your travels? Who are you staying with? How do you know that person you're staying with (if you didn't say a hotel, etc.)? Have you ever had any interactions with the police? (We think it's a gamble to lie about criminal records.) Have you ever been arrested? What were you arrested for? Have you ever smoked weed? Do you have a return flight? Can I see the information about your return flight?

The questions they ask you in secondary inspection will be determined by their reason for detaining you. They may just be searching your vehicle, or want proof of your residence/employment in your country of residence. They may want you to fill out a customs declaration card with a destination address and home address.

In secondary inspection, they also may ask for your phone, email, and Facebook/social media. Consider that if you're being asked for social media and email information, it could be a sign that they are targeting you for intelligence gathering. If/when this happens, this is likely your cue to stop talking, especially if you don't have "clean" accounts set up.

When other people's names come up in questioning: this leads to a likelihood that there could be a larger investigation going on, and you don't know what they already know. Unless you have previously spoken with the person they asked about and explicitly agreed on what to say about each other at the border, say nothing. "I don't know" and "I don't remember" are good options, as well as "I'd like to speak to my lawyer". Remember that they are professional interrogators. It's really sketchy to think you can "outwit" your interrogators and/or the police, and it's really hard to stop talking once you've started.

Phones and electronic devices

> "They want to get information from us by using our technology, and if they get access then they can often get more information about our networks than from an interrogation."

Phones and electronic devices are a huge problem! Even ten years ago, it wouldn't have been strange to not own a cell phone. Now, not having a phone is suspicious, and it's reason enough to question you further. We know the U.S. border has denied people who have: given them full access to their phones, refused to hand over their phones, showed up with factory reset phones, and who were traveling without a phone.

Fortunately, there are options available to us for when we're crossing the border with phones and other electronic devices. As with all tech security, none of the encryption or other techniques described below are going to provide guaranteed protection. However, they do greatly increase the chances that border guards will not be able to access the phone. Also, all of these options still completely depend on no one disclosing the password to their devices at the border.

The most important thing is to never cross the border with a phone, laptop or tablet you regularly use without encrypting it first. If it is not encrypted then it will be easy for the border to read everything on it. iPhones are automatically encrypted whereas Android phones need to be encrypted by going into the settings and enabling it. There are various options for enabling full disk ecryption on Windows, Mac, or Linux. This is a good tech security practice anytime, but it should be mandatory for crossing the border with your phone or other device!

A second important thing is to turn off your devices before crossing the border. If they are turned on, there can be ways to bypass the encryption. An encrypted, powered down device is the best chance we have to protect our digital information from the State.

On SD cards: If your phone has an external SD card, this needs to be encrypted seperately. Some phones may not have an option to do this, in which case the SD card should be removed and left behind.

Once the storage on a device is encrypted and the device is turned off, typically the only way to get access to that data will be by guessing the encryption password.