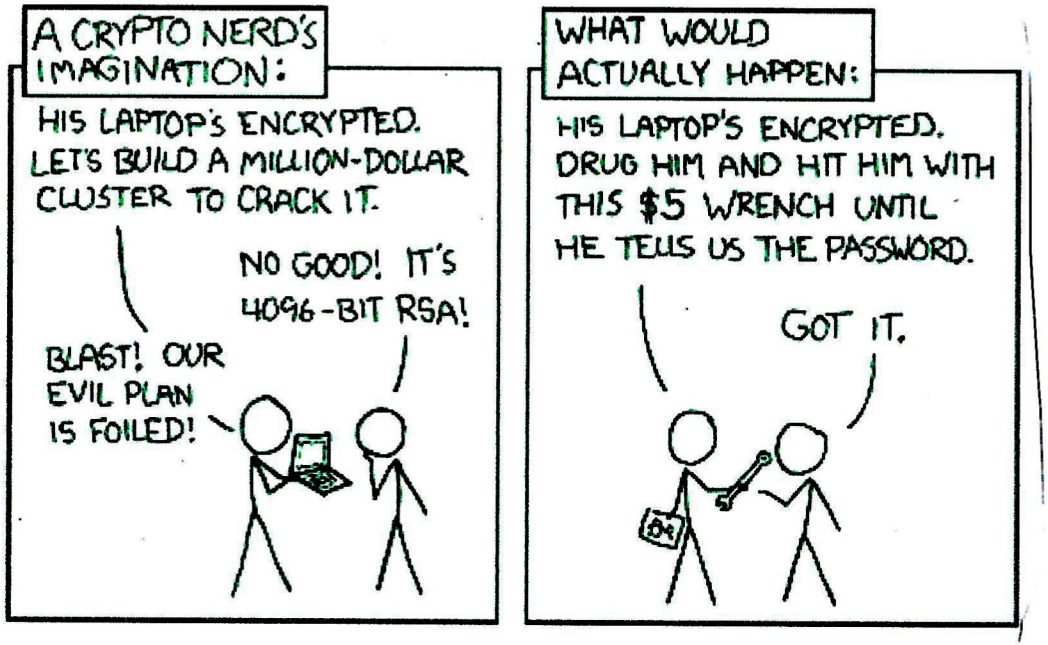
CASE STUDY: Prarieland Antifa Trial, $5 wrench and relational security

Over in our fellow fash settler colony of Amerikkka, following Trump designating 'antifa' as 'terrorists, eight non-cooperating protestors have been convicted by the state in 2026 on serious charges, including material support of 'terrorism', over an anti-ICE noise demo. In reflecting on the trial, supporters stressed the state's effective strategy of using the "$5 wrench" versus say a supercomputer / cellebrite to try break encryption, as the weak link that won people over to snitch on their comrades.* The state's wrench relied on psychological pressure and threats of violence in prison to get people to turn on their friends.



Despite the state spending extensive resources on digital extraction requests going back to 2021, the most sensitive information came from people who quickly co-operated with the state by giving their devices and passcodes to the cops. This snitching betrayal by some people (who still are doing time in cages without the support of radical networks) enabled the state to obtain signal messages that they otherwise could not get, leading to the conviction of themselves and eight non-cooperating defendants.

*"You can be as encrypted as you want, but if you're talking to someone who's going to snitch, then it doesn't matter. And that type of relational security as opposed to technical security is what really keeps our movement safe."**

*Search for 'Outlaw Podcast', Prairieland Trial Reflections with Lydia & Lee, March 27, 2026.

CASE STUDY: telecommunications request costs in a multiple murders case

In one example of limits, in a high-profile multiple murder case in 2025, Victoria police revealed it was "cost prohibitive" (> $100k) to obtain location-based phone data for a year for the accused. Instead, police budget constraints only allowed them to pick individual dates. Any app you may have that records your location (ideally you don't have) is far easier for the police than obtaining long time periods of "Event-Based Monitoring" telecommunications data.

If you give your passcode, the police will also see you as a potential 'weak link' to further harass and follow up for more information. It's best practice to not have 'anything' on our phones but the reality is they are still very compromising in digital world we spend so much of our lives behind a screen.

'Nothing big to hide' downplays how relational our political networks are and therefore vulnerable to extra relational stresses. The state knowing all our innocuous associations, community drama and gossip gives the state information that can break our networks. Navigating our differences already requires all our skills without the state weighing down on manipulating our weak points to break them!

^ Read the UK Zine '[illegible]elf Defence' for an introduction: https://digitalselfdefence.net/, and the zines at Zine Squatte Shoppe: https://zinesquatteshoppe.noblogs.org/category/tech-security-guides

#On that note turn off AI on Android / IOS that reads over text on screen including disappearing messages, enabling a way for police to read expired messages, which may be stored in plain text for a week (this happened with Disrupt Land Forces phone seizures).

Giving your password to the cops gives them the most information for their harassment of us in the least time, which emboldens them and maximises the chance of them obtaining sensitive, incriminating information.

It is true that 'israeli' spy tech Cellebrite breaks most phones encryption eventually (GrapheneOs is generally an exception, we recommend)—but it does take time and resources depending on device updates, power status and passcode lengths. Creating time allows for disappearing messages on encrypted apps to self-delete. Further, time stretches cops to internal money and resource limits they have on investigations.

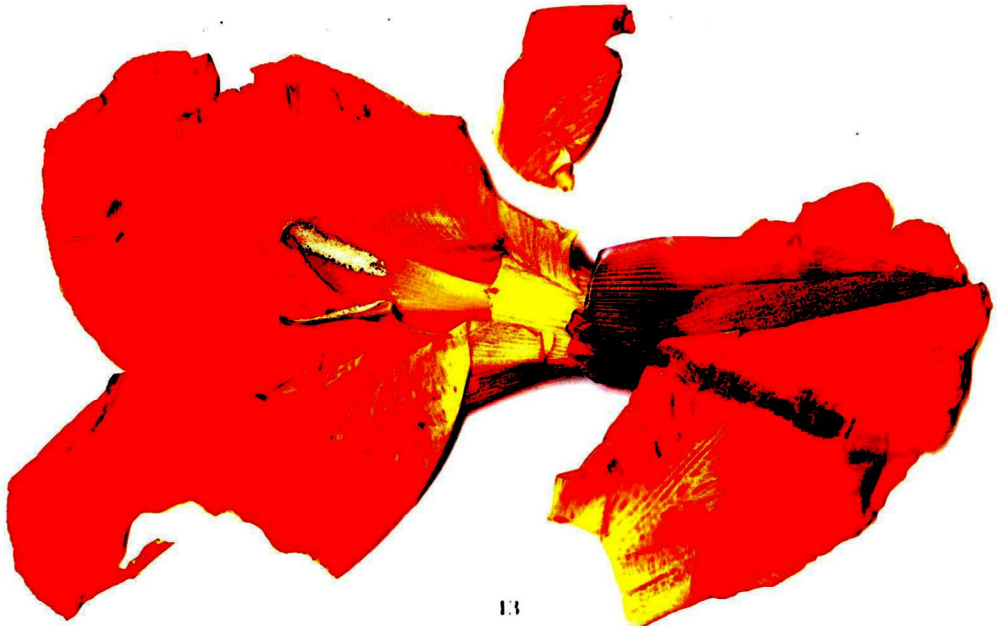
Underneath this justification of 'nothing to hide' / 'it's too hard' are liberal assumptions and feelings of defeat that fall into a kind of 'security nihilism'. These justifications over-emphasise the power of the state, and under-emphasise our collective responsibility. Security with one another is collective solidarity, no matter how 'important' or not you deem the information to be, or 'how much they already know' about you.

ASIDE: Beware crossing state borders!

When crossing borders you can expect possible harassment from 'Australian Border Force' or other authorities who have extraordinary power re: stop, inspect, seize and detain. In the 2 years to 2024,* one quarter of people stopped at the border had some data copied from their devices (94% of people provided a passcode despite there being no legal requirement).

At the border, cops use the legal threat of seizing the device to make people 'voluntarily' give their passcode. In anticipation of this, you may take a new device that has never had any personal information on it. Despite the pressure they use at the border, authorities cannot charge you for not unlocking your phone unless they have a warrant / suspect it holds evidence of a crime.

*-https://www.theguardian.com/australia-news/article/2024/jun/11/australian-border-force-abf-searching-phones-travellers-data



Justification: the lawyer I talked to told me to give my passcode over to the cops.

Reality: Lawyers are bound to the court, so they will recommend compliance. We do not believe in the criminal legal system and instead have radical political commitments and trust with each other to uphold.

Lawyers are bound to different principles than us. They have sworn to follow the law and put the best interests of the 'court and administration of justice' above their clients if those interests are in conflict. Because of their principles they will generally recommend you give your passcode to the police if they have a valid warrant because to do otherwise would be to recommend you commit an offense. In contrast, we have radical collective interests and commitments against betraying each other's trust by giving sensitive information to the state.

Our personal and political goals conflict with the legal goals of our lawyer on sharing passcodes with the state. Personally, we have confidential information we've shared with close people in our lives which is violating for the abusive state to know. Politically, we want to advance radical struggle, which means using our power to refuse to give them information about us and our comrades, they can use to repress us.

For more information on the differences between personal, political and legal goals, we recommend reading: *'A Tilted Guide to Being a Defendant: A Guide to the Criminal Legal System for Radicals'* Chapter 2, pp. 39-83, available at libcom.org and Zine Squatte Shoppe.

Justification: The state already can already request all my data / metadata. Cellebrite can crack my phone anyway. I have nothing big to hide / it's too hard to keep things secret. I should give my passcode to avoid a charge.

Reality: We have a lot to fear about what is on our phones. Any friction we can create that makes police investigation of us slower and harder builds collective trust and safety. Co-operation with cops sabotages collective trust, and provides an entry point for cops to demand ongoing co-operation from you.

It is true the state has wide-ranging warrantless access to digital metadata: SMSs, to phone call times are all easily accessible. Phones are tracking devices. Under a warrant, the state can request telecommunication companies for location access and send access requests to corporations about accounts under names they know about. Even without a warrant, apps that rely on advertising that you've granted location permission may sell your data to advertising data brokers that the state can then buy.

All these tools the state has takes extra time and resources that may face severe limits (see case studies). They are not as direct for many things as getting full access to a phone via an instant password. We can also combat many of the state's tools by spreading information on Digital Security such as hardened phone settings, strong passcodes, encrypted messaging, Tails OS, to use of VPNs. (Links at end of section!)^

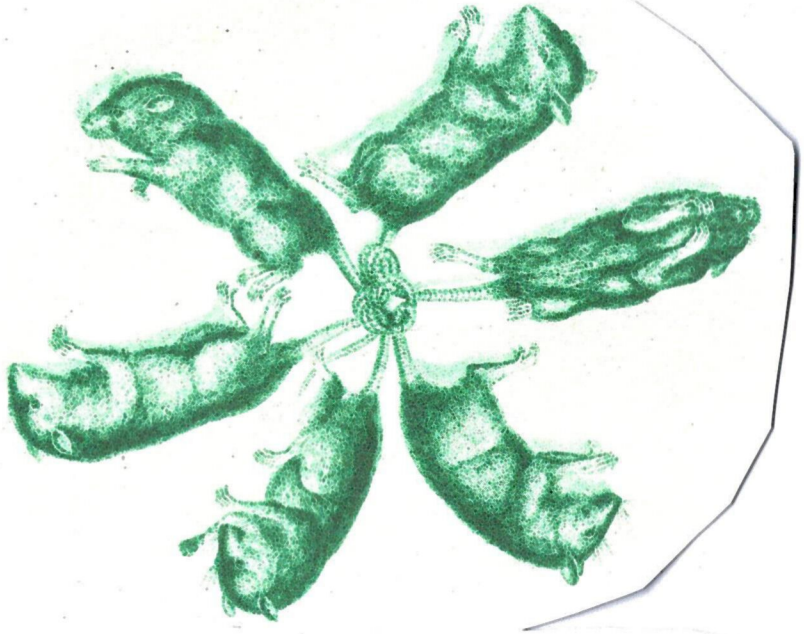
CASE STUDY: Disrupt Burrup Hub and perspective

Media co-ordinator Jesse Noakes, from Disrupt Burrup Hub, avoided jail time from four charges of refusing to follow police directions to give his passcodes in 2023, in 'western australia'. He was found guilty, ordered to pay a $1000 fine and $137 in court costs. The campaign opposed fossil fuel giant Woodside's destructive gas terminal on the Burrup Peninsula, which damages Murujuga rock art and landscapes.

The same charges often comes up in relation to cops criminalising illicit drug business networks to planned acts of violence. In these cases, according to public case notes, people have been locked up for a month of two longer. However, the passcode charge is a small fraction of the more serious charges that led to years of jail time for these people.

Snitching is carceral: against snitch culture

The rat makes a wager: "maybe the state will take less of my life-time if I give them the means of taking the life-time of others." It is the very logic of competition that emanates from the essence of capitalist social relations.—Richard Hunsinger, George Floyd Uprising former political prisoner https://www.abcf.net/blog/on-cooperators-their-sympathizers/



The word 'snitch' is believed to originate in 17th century Britian, as underworld slang, coming from the word 'snout' : someone on the nose as an informer to the cops. Snitches get stiches! Anyone that betrays our trust by talking to the cops is a danger to our struggle. We need to have expectations on what happens with snitching. And we need to combat the interests that lead to people snitching.

map you and your networks. You may avoid a passcode charge but end up with others, including to people close to you in your network. You will also then have to deal with the fallout from a loss of trust and connection with your comrades.

Crimes Act (1958) Vic

Under Sections 465AA and 465AAA, the state has the violent power to charge people for refusing to provide their passcodes without a valid excuse. 465AA is via a court order (5 years max prison) and 465AAA is via a police officer's direction (2 years max prison). There are similar Federal laws, and state laws across each jurisdiction.

Fear: If I don't give the cops my passwords I will go to prison.

Reality: Passcode charges often get dropped. Even when pressed, in the current context, it's unlikely you'll go to prison on that charge alone. Doing any form of political activity means facing the reality of risk of imprisonment.

It is true that police, if they have obtained a warrant, have the power to charge you for refusing to follow their direction to unlock your devices, which comes with a prison sentence as a possible outcome (See Crimes Act at end of section). We have seen again and again, police in a raid weaponise the psychological threat of prison to manipulate us to give them our passcodes. A charge does not necessarily mean you go to prison—it will go to court where we can support you and fight it together.

A maximum sentence for any charge is the worst case scenario that happens in the worst of cases. Prison (likely to be far less than the max) may be possible but especially if it is the only charge you have at present, it is far more likely to be other possibilities: including fines and undertakings. Furthermore, fighting the charge may mean the police have to drop it, including by challenging the legality of the police's actions.

The fear of going to prison may be real but it is not addressed by giving your passcode. More importantly, the risk of prison started long before any cop threatens any of us with a passcode charge. In doing any form of resistance work, we have to understand prison is a risk for us.

Giving your passcode means you have voluntarily given the police information about you and your comrades they can use to criminalise and

Giving your passcode to the cops is a form of snitching. What we should do when someone betrays our collective trust needs to be informed by our collective values. We need to talk in our collectives about what are appropriate consequences for snitching, right-sized for the degree of harm it causes in each case.

Some may push back and want to centre 'individual choice' to co-operate with the state and view consequences for snitches as 'carceral'. What is at stake is not an individual choice. It is a choice that puts collective struggle at risk.

As we saw in the Prairieland Trial overseas this year, snitching sends people to prison. This includes the imprisoned snitchers, who now face the additional consequence of not having the support of radical networks while facing years in prison.

There may be tactical exceptions re: giving phone passcodes, such as completely blank phones that everyone is aware about beforehand. But these exceptions are not what we are criticising in this zine.

What we are critiquing is individualism triumphing over radical collective trust. We see individualism championed through the NGOisation of resistance, which benignly promotes co-operation with the cops, rather than defying unjust laws.

This is matter of political survival when we believe in mass anti-colonial class war. There are more of us than our political enemies—but not when some of us do the work of police giving them confidential information. Suddenly, we're fractured and exposed to further repression.

The zine '*Coping with Snitch Culture Historical Examples Current Proposals*' goes through examples of what's worked and failed in tackling snitch culture in various radical struggles.# Two of the ways to combat snitch culture they highlight are shared community expectations and consequences, and prisoner solidarity.

As revolutionaries we are against the criminal legal system. To do so means grappling with real risks. Instead of pursung 'innocence', we can see ourselves as all to varying extents 'criminals' / enemies of the state, while being mindful of material differences across race, gender, class, sexuality and ability.

What may also be underlying attempts to avoid a charge on passcodes is a feeling that you will not be supported by comrades through a legal process. The criminal legal system is a system of isolation and punishment, with very mystical bureaucratic legal theatre. We can combat the real isolation caused by the system through court solidarity with defendants and material prison solidarity.

breaks the trust we have with each other by not putting collective security first.

We write this zine because we have seen too often the state exploit a lack of seriousness in our networks of the gravity of giving our passcodes to our enemies.

Here we go into how we can collectively fight the fears around cops criminalising us for refusing to give our passcodes. We share some case studies. We break apart some common justifications that creates pressure to give passcodes to cops. And we touch on consequences and breaking snitch culture.

Why we refuse give passcodes to the state!

Our digital devices have extraordinary levels of private information about us and our networks. They show who we're closest to and where we have been. They show all our photos, including of our friends. They show our messages and calls. They show our documents that we share together. They show our digital finances.

As comrades fighting for revolution, our strength lies in the collective trust we share together. The less the state knows about our relationships, the more we are able to stay safe.

The state uses the repressive tactic of device confiscation to criminalise us and map our networks. Giving your passcode to the cops is a form of snitching: giving the state sensitive information on you and your networks. Unlike other tactics the state employs, we have complete control over giving our passcodes to them.

Every successful revolutionary movement values building collective loyalty to each other in struggle. On the flipside, this means cultivating a collective culture of non-cooperation with our political enemies, including the cops. We have a responsibility to talk about this with each other, including those newly politicised, so we are on the same page.

Not giving your passcode follows the same collective principle as 'no comment' to all police questions except your name and address in a first police interview.

Handing over your passcode shows your willingness to co-operate with police investigations and provide valuable evidence for the police. It

Such solidarity means not just showing up at the court date. It means support around material impacts including loss of jobs, mental health support to debility from injuries. It means political defence campaigns. It means letter writing to those inside prison. It means counter-repression: hitting back at the state to inflict a higher cost on the state hitting us.

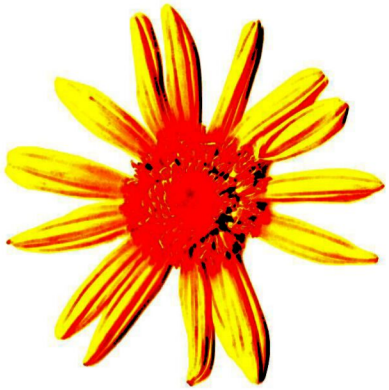
In general, the state paints those it has criminalised as 'bad' vs the supposed 'good' people who follow the law. We can challenge this liberal binary by actively being in solidarity with criminalised people in and out of prison.

As part of that solidarity is nurturing more mutual aid with each other to strengthen relationships. Building this community infrastructure must be interweaved far beyond small radical circles, to show we are invested in a struggle far bigger than us, to radically transform society.

The simple act of refusing to give your passcode to the cops seems small. But it has big ramifications. Instead of individualist acts of betrayal damaging our ecosystems. We grow stems of trust that flower into seeds of hope for revolution.

$ (Jonathon Green (2012), Crooked Talk, Five Hundred Years of the Language of Crime - Page 255).

#Access: https://www.southchicagoabc.org/zine/abc-Coping-with-Snitch-Culture-Historical-Examples-Current-Proposals/



DO NOT GIVE YOUR PASSCODE TO THE COPS!

Anon zine released from the lands of the Eastern Kulin nations, known as the occupied city of 'melbourne', in April, 2026. Find an electronic version at: https://antieverything.noblogs.org/ &
https://zinesquatteshoppe.noblogs.org/