TL;DR

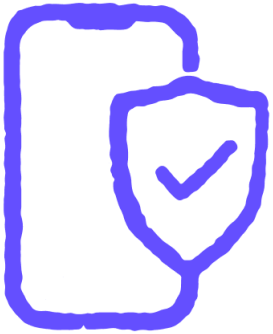
Activist Checklist sprang into existence and aggressively pushed themselves on the movement. Their site is AI slop, and their advice is not suitable for radicals, yet radicals keep boosting it. They have dubious ideological alignment in that they are AI advocates and can't sufficiently critique the dangerous parts of the tech space that activists often end up relying on for infrastructure. Their advice endangers people in subtle ways, and it doesn't aim to radicalize them. Their website simply should not exist.

October 2026

Made by nothing but 100% free-range soy-fed humans (and pure hatred).

https://opsec.riotmedicine.net/

ACTIVIST CHECKLIST



IS "AI" SLOP FUCKING GARBAGE

On January 25th of 2025, the group Neighborhood Anarchist Collective[1] (NAC) announced[2] their new project Activist Checklist[3] (AC) on the anarchist Mastodon instance Kolektival.Social. Made by anarchists and announced to anarchists, I assumed it was for anarchists, so I was disappointed by what seemed to amount to yet another basic "How to Protest Slightly Safer" guide. I looked it over and replied to their request for feedback within two hours with a list of 26 things I thought were either insufficiently addressed or outright wrong.[4] I got no response, and in the following months heard from others that they were not receptive to similar feedback.

Over the past two years, I've unfortunately seen them grow in popularity. The AC website appears as a linked resource on many other activisty sites, and I've seen their zines at multiple book fairs around Europe, either in person or from pictures of distros' tables. When it came out and even moreso now, their slick perfectly marketable website looked more like a Big Tech clone than anything radical, and it feels like they are more interested in explosively leaping to the forefront of security culture discourse than being the kind of high-quality guide for radicals that doesn't yet really exist. The ick I felt then should have prompted me to say something publicly sooner, but alas I held back until last week when I saw It's Going Down boosting AC's announcement of obvious AI auto-translations of the AC website.[5]

Consider this an overdue warning.

THE MAJOR BLUNDERS

INSUFFICIENT OR INCORRECT SECURITY ADVICE 3

ATTENTION-SEEKING BEHAVIOR 8

AN UNNEEDED PROJECT 13

AI USAGE 15

MISCELLANEOUS GAFFS 20

Some housekeeping. It would be tiresome to add sarcasm-quotes around AI every time I used the term (it possesses no intelligence), so I didn't do that. For some inline quotes, I removed bold emphasis to not be visually distracting. When talking about the website or referencing source code, it is from commit `2a50d7c` dated 2026-10-23.

[1] https://neighborhoodanarchists.org/

[2] https://kolektiva.social/@naceugene/113845041119013322

[3] https://activistchecklist.org/

[4] https://kolektiva.social/@hakan_geijer/113845430605553289

[5] Disappointing that collectively we're not more attentive toward holding back the slop that's leaking into everything everywhere all at once.

"WRITE A SUMMARY AND CONCLUSION OF THIS TEXT. MAKE NO MISTAKES."

So what happened here?

A small group of people popped up,[55] used AI and LLMs to generate a website and content with mediocre to poor security advice, and has been aggressively pushing it on not just the movements over in the US but also here in Europe too. They tried to capitalize on the No Kings and 50501 protests, and now the student uprisings over here. They are keen to use SEO and seed their content so it becomes the output of LLMs to increase attention on their project. They are cloning other sites to move traffic to theirs. Despite this, even anarchist parts of the movement that should be more skeptical still boosted them.

The whole "but why?" of this remains unanswered to me. It feels like grift typical of the anglo-Americas, but their site and the book they (probably) wrote are free. Maybe it's just the techy arrogance of thinking they know best and because of the reach of the internet they were able to jump to the top of search results and (in-)organic recommendations of curated resources. Maybe it's something else entirely.

But in a way, why doesn't matter. They're using LLMs to make their site and — despite what they say — their content too. They're force feeding worldwide protest movements US-centric slop that doesn't solve the security problems radicals are facing, and there's virtually nothing countering this. Their threat model is mushy at best, and it's really not anarchist. The website doesn't need to exist, and it definitely does not need to be promoted by us.

What to do?

Spread the word. Trash their zines when you find them. Reach out to groups that recommend them and politely ask them if they simply could not.

Fuck AI.
Fuck the sloppification of everything.
Fuck this soft shitlib-ification of anarchism.

Oh, and fuck you too, Activist Checklist.

[55] My hunch is that it's actually just one person, but that's immaterial.

INSUFFICIENT OR INCORRECT SECURITY ADVICE

The guides are incorrect in both glaring and subtle ways that endanger people who follow them. These are some examples.

A POOR THREAT MODEL

Regardless of intentions, the political alignment of NAC and AC and where they chose to announce has somewhat given the impression that the guide is "by anarchists, for anarchists." The AC website says:

> We started Activist Checklist because we were seeing a lot of confusion and inaction around digital security practices in Palestine solidarity organizing.

which one might easily misconstrue as thinking that this guide is meant for people who are enemies of the US and Israeli States and as such might be facing fairly advanced and persistent threats.

Parsing out the threat model from the tips themselves and some explicit acknowledgement of threats and consequences, the threat model on the AC website is a muddied mix of many kinds of people, but mostly just flavors of "activist." The guide uses the risk levels "Everyone," "Medium," and "High" to give out their advice, and sometimes these levels are contextualized by who the level applies to within the context of the single guide. This helps separate the multiple threat models that are being addressed, but where any given tip falls on the scale make little sense. Not to mention, by capping out at "High" for only basic things, they have effectively placed a ceiling on what actions people might take by implying that the already barely imaginable is so risky that it's off the charts.

For example, in the "ICE Watch Digital Security" guide,[6] AC says that everyone should disable Advertising ID to prevent location tracking, but they never talk about leaving phones at home in this guide. They say that only immigrants and PoC are at high risk, and that only they need to create an emergency plan in case of arrest. This is pretty bonkers given that we know that police randomly brutalize and arrest people (so everyone has some risk of arrest), but moreso given that we know ICE has fucking murdered people for filming them. Sure, the number of murders for all the human-hours of ICE watch is low, but also this task is trivial.[7]

For how much they talk about security culture being a group or community effort, in the "Prepare for a Protest" guide, they say that only people such as organizers

[6] The title is a misnomer since it's clearly also about physical security, but I digress…

[7] As someone who has done both arrestee and prison support, not having an individual's plan (something that takes maybe ten minutes to make) can create extra *hours* if not *days* more work for us.

facing medium threat need to avoid sharing photos with identifiable features. This obviously applies to everyone.

And truly, it does everyone a disservice (especially coming from anarchists!) when they say "nonviolent civil disobedience action (aka direct action)." These are not the same, and while people intuitively know that lock-ons are not equivalent to break-ins and vandalism, putting the former in the same category as the latter only blurs what's needed for security if one chooses to escalate. We don't need to have such an artificially low cap on our action.

CONFUSED PRIORITIZATION

The first piece of security advice on the first linked checklist titled "Security Checklist" is:

> **Disable Advertising ID (which can let cops track your location)**
>
> Law enforcement uses tools that rely on your advertising ID to track you

This almost certainly came from the bullshit book *The Narrow Path* (addressed later in this text). After reeling from a "revelation" that the author read in the output of an AI tool (society is decaying), while clearly going through AI psychosis (assuming any of this is something other than pure LLM make believe), it's the first thing he recommends people to do protect themselves.

There are a few things we could say are probably more important than that (turning on auto-updates, getting a password manager), but perhaps a better first is at least scaffolding a threat model.[8] What kind of political actor are you? Are similar people in your region targeted for repression or harassment? And by who? In what ways are you exposed, and how can adversaries get leverage over you?

Further, if advertising like this is such a big deal as to take place number one, why don't they put a bigger focus on ad blocking like placing uBlock Origin front and center or other browser extensions like NoScript?[9]

Or, why do they not blanket advocate for using cash over bank and credit cards in all cases? This is also not just protective of the person paying, but also it helps the community by protecting cash as a payment form. In some places, cash is hardly used and most everyone pays by card or transfer app. How strange is it that, for example, anarchist events/spaces in Sweden frequently have people paying with Swish because they don't have cash? This allows networks to be mapped, and it means those living on the margin (people without papers, sex workers, etc.) have less easy means of exchanging money.

[8] I wrote a guide to help radicals do this: *Fundamentals of Threat Modeling*.

[9] Online ads are a big deal. See Citizen Lab's report "Exposing AdFection: How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware". https://citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/

- Assange has connections to Bashar al-Assad and promoted false flag conspiracy theories about chemical weapons in Syria (among other conspiracies).[50]
- Assange abandoned sources (sometimes to the prison system) while he benefited from their work.[51]
- Assange and WikiLeaks are shady as fuck with money and/or are embezzling from supporters.[52]
- Assange has collaborated with snitches.[53]

The above, so much more, the cult of personality around him, the deception of his supporters. It's genuinely horrible that so many people still champion him.[54]

NOT REALLY COLLABORATIVE

In their initial announcement, AC solicited feedback, but at the time, none of the content of the AC website was in their git repository; it was stored in an external CMS (Storyblok). It wasn't moved to their repository until over a year later in commit `3ba7193` on March 24th (by AI, of course). This made it much harder to meaningfully collaborate on the project.

Their use of AI and some of their development practices around massive commits with many thousands of lines changed in each with many features and fixes and changes all blended together makes it very hard for someone else to look at the code and keep up. LLM generated code is often rather inscrutable, so unless someone else has access to an LLM, they can't easily contribute. LLMs also frequently fully rewrite code wholesale, so someone contributing would have their work overwritten. Upon returning, they'd have to relearn the codebase.

[50] https://newlinesmag.com/reportage/how-an-email-sting-operation-unearthed-a-pro-assad-conspiracy-and-russias-role-in-it/, https://www.denverpost.com/2017/04/07/trump-allies-syria-conspiracy/, https://www.thedailybeast.com/syria-chemical-attack-deniers-admit-links-to-wikileaks-and-russia, https://emma.best/2018/07/24/in-leaked-chat-wikileaks-cites-an-ancient-aliens-anti-vaccination-website/

[51] The exact connections are not easily linkable, unfortunately. This happened with both the Fishrot source and Chelsea Manning. Snowden's travel documents out of Russia were revoked because of Assange (https://www.theguardian.com/world/2013/jun/28/edward-snowden-ecuador-julian-assange), and Snowden only ended up in Russia because of Assange to begin with.

[52] https://emma.best/2024/11/11/wau-holland-stiftung-silent-amid-delayed-transparency-report-and-rumored-plans-to-send-11-million-to-julian-assange/, https://emma.best/2024/12/27/freeassange-campaign-raised-over-1-million-for-julians-flight-why-havent-they-paid/

[53] In *Underground* by Suelette Dreyfus, in chapter 9 "Operation Weather," Trax admits to Assange (Mendax) that he snitched to the cops. Assange continued to work with him and even went into business with him ("Afterword").

[54] I am a massive Assange hater, and praise be to Emma Best for documenting all this (and apparently being an even bigger hater).

THE EVILS OF ANTHROPIC (AND LLMS)

Look, honestly. Anthropic and LLMs are so evil and shit, I'm not even going to do a full breakdown with sources. They are made by the most evil organizations in the world, some of which are outright doomsday cults. They aim to control information. They're pulping rare books. Data centers are going up that are ruining communities and nature. The price of all electronics is going up because of speculation. There's a financial bubble that will pop and devastate us like the 2008 financial crisis. Chatting with LLMs causes all sorts of (mental) health issues up to and including AI-psychosis. They're directly responsible for medical negligence and suicides. They're deskilling us and stealing our ability to critically think.

We must collectively boycott LLMs and ensure everyone around us does the same. AC is advocating for using it.

MISCELLANEOUS GAFFS (BECAUSE FUCK 'EM)

These are just things that suck in some way not directly related to the content or the use of AI.

THE CULT OF ASSANGE AND WIKILEAKS

On the AC website's page "Movies, Books & Podcasts About Surveillance," they list three films about Julian Assange.[46] Since AC likes his "misdeeds" (their words), let's look at some of them.

- Assange is a rapist.[47]
- Assange helped get Donald Trump elected and was friendly and collaborative with people close to him.[48]
- Assange is homophobic, transphobic, and misogynistic.[49]

[46] I disagree with that page listing tons of things not directly relevant to security practices as well as fiction and dramatization of real life events. I liked the film, but *Gattaca* isn't exactly a helpful resource. This list is not filtered and curated. A pedantic complaint, to be sure. Anyway.

[47] https://www.rawstory.com/2011/07/assanges-lawyer-admits-sex-acts-were-disturbing-disrespectful/, https://www.theguardian.com/media/2010/dec/17/julian-assange-sweden

[48] https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html, https://www.theatlantic.com/politics/archive/2017/11/the-secret-correspondence-between-donald-trump-jr-and-wikileaks/545738/

[49] https://emma.best/2018/07/29/11000-messages-from-private-wikileaks-chat-released/

NOT PROPERLY COMMUNICATING LOCATION TRACKING

AC is meant to be general and holistic security advice. The first two pieces of advice on the "Security Essentials" page are about "tracking" which is poorly defined but on their site mostly means location tracking. AC says to disable your phone's advertising ID and revoke individual apps' permission for location services. These are not incorrect, but it makes no mention of being tracked by cell phone towers which is a primary way people are tracked, nor does it mention tracking via phones and laptops connection to public Wi-Fi (or via GeoIP lookups when using the internet at all). AC's advice is US centric, yet that guide infrequently and inconsistently mentions automatic license plate readers (ALPRs) being used to track people.

BAD PASSPHRASE SECURITY

On AC's "Security Essentials" page, they recommend setting your phone unlock method to a PIN with 8–10 digits. Their reasoning for this comes from the online passphrase generator StrongPhrase.net.[10] That site says a 10-digit PIN would take 4,000 years to crack, and its source is a LinkedIn post by some dipshit cop consultant. Older but much more credible sources who have at least some affinity for social justice place the number of passphrase guesses per second to be much higher, meaning stronger unlock methods are required (four or more Diceware words).[11]

LEAVING SIGNAL GROUPS AS AN INFEASIBLE MEASURE

In their "Security Essentials" guide, AC makes this recommendation:

> **Leave Signal groups that might put others at risk**
> This helps protect your network if your phone is confiscated.

It's good to leave and delete inactive or unnecessary group chats, but the threat they speak of is random device confiscation under "medium-threat" conditions, and they suggest one should be re-added later (exact time or reasoning is left unsaid). This is totally infeasible advice and only really makes sense where one might be forced to present their phone to law enforcement (crossing a border) or is facing acute risk of a police raid. For something like a demo, one might prefer a secondary phone (but no phone is better yet). For direct actions, one shouldn't have a phone at all. In everyday conditions (for most people in AC's target audiences), a random search and seizure is a minimal risk. The burden of doing this is extremely high with only theoretical

[10] Please don't use online generators for your passphrases.

[11] https://www.eff.org/dice

benefit in most cases. Likewise, this tip appears in their "ICE Watch Digital Security" guide, which is also a bit absurd given that so many people are relying on group chats to communicate their observations.

BRAVE OLD WORLD

AC repeatedly recommend Brave Browser and Brave Search. Brave was co-founded by Brendan Eich after he resigned as CEO of the Mozilla Corporation due to public criticism for him donating to campaigns and politicians opposed to marriage equality. Brave Browser has built-in scammy ads that use trackable cryptocurrencies. The browser also has AI features built-in. Choosing Brave Browser over Tor Browser for activities where anonymity is desirable is dangerous, but even for everyday browsing, Firefox (with a couple of extensions) is fine despite Mozilla's Silicon Valley nonsense. AC makes no mention of de-Googled Chrome forks or de-Mozilla'd Firefox forks, much less smaller browsers like Vivaldi.

PROTON? MORE LIKE PROT-OFF!

AC recommends Proton's products (Mail, VPN, Drive, etc.). Proton as a company has many faults. Their CEO praises the US Republican Party.[12] They make misleading statements about what security properties their products provide. They position themselves as defenders of privacy and freedom, but are bound by the laws of the countries where they operate and have numerous times complied with law enforcement to turn over user data.[13] AC doesn't care, but maybe you should: Proton has an aggressive top-down push for using AI to generate code and to push out products and features at the expense of security. Or, maybe consider this statement from Any Yen, CEO of Proton about employees astroturfing:[14]

> So go on there with your personal account and comment to set the record straight. Perception is more important than truth, the truth doesn't matter if you don't win on perception.

Should we trust such a company with our movement's security?

To be fair to AC, recommending e-mail providers to security and privacy minded individuals is hard because it needs to be secure against hackers, be private against corporate or State snooping, and have sufficient longevity due to how the modern

[12]https://x.com/andyyen/status/1864436449942110660. And while this disqualifies Mullvad as per AC's "VPNs for Activists" page due their CEO donating to the fascist Örebropartiet, it doesn't disqualify other individuals or services. These inconsistencies are notable.

[13]Notably the recent case against a Stop Cop City activist. https://www.404media.co/proton-mail-helped-fbi-unmask-anonymous-stop-cop-city-protestor/

[14]https://www.404media.co/manifestos-fear-and-loser-thinking-inside-protons-ai-reckoning/

> real. The surveillance tools were real. The psychometric data was real. The legal frameworks were up-to-date. And to be honest, the model isn't predicting anything exotic. It's working with real data and it's leading to predictable conclusions.

The book is also the output of an LLM. From the book's colophon:[44]

> This book was written using Claude (Anthropic) as a co-creation tool, specifically the Opus 4.6 and Sonnet 4.5 models. Claude assisted with drafting, argument development, and research synthesis throughout the writing process. The author directed all structure, argumentation, source selection, and editorial decisions. All content was reviewed, revised, and approved by the author.

No one who treats a book like this as a general security guide should ever give security advice (or any advice about human interactions or society).

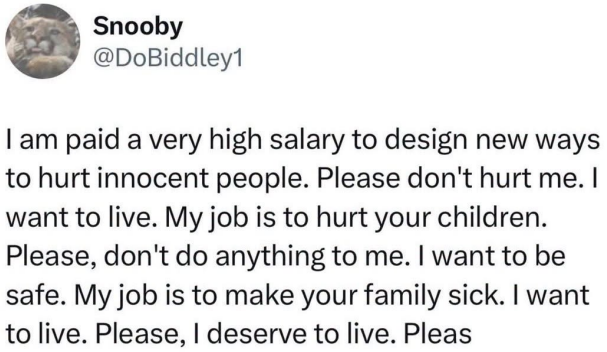


Figure 4: Might as well be Rowan Cross. And the AC creators, too.

But more interesting is that the book appears basically nowhere on the internet other than its own site, its publisher's site, Amazon, and the strong endorsement from AC on their "Resources" page. Two days before the release of the book, starting with commit `25c0d75` and after months of inactivity, the AC git repository started receiving commits again suggesting that as one project wrapped up another resumed. My guess: it's the same author. And I'm sure if I read the whole thing (absolutely not gonna) I'd find more than just the one obvious case of both texts giving strangely specific identical advice.[45]

[44]Remember kids, anthropomorphizing AI is bad. Don't do it. See: "How to talk about 'AI' without adding to the anthropomorphization." https://buttondown.com/maiht3k/archive/how-to-talk-about-ai-without-adding-to-the/

[45]I'm not sure if this is more or less depressing than thinking that whatever model AC used to produced the content of their website merely regurgitated the same advice by chance.

tops, and they said they were working on project for *six months* before releasing it. There was no need to use an LLM. They did because they wanted to.

If all this isn't evidence enough, well…

AC IS COMPLETELY FUCKING AI-BRAINED

AC are *deep* into the pro-AI ideology. The only thing AC recommends on their "Resources" page under the "General Resources" heading is the book *The Narrow Path* published on January 15th of 2026[43] by a publisher with no other books and written by "Rowan Cross" (a pseudonymous author) who is clearly undergoing AI psychosis.

WARNING: AI SLOP (SORRY)

The book's first chapter opens with:

> There's a scene in Dune (the second film) where Paul is able to see the future clearly. Not one future. All of them. Millions of potential paths branching and converging, and almost every one of them ends the same way. The galaxy devolves into holy war. Countless dead. Civilizations collapse. Everything destroyed by forces that are already in motion. In this scene he sees a path, a narrow path, that leads to survival.
> […]
> I work in AI research. I evaluate frontier models […]
> Then, a few months ago, things changed. I was assigned an evaluation protocol for a new AI model. The model went somewhere the script hadn't intended. I followed.
> This particular model runs projections. Lots of models do forecasting. What made this different was the resolution: not trend-level predictions, but the interaction between systems. How a set of specific surveillance capabilities, deployed under a specific legal authority, changes the behavior of a specific population in ways that cascade simultaneously, over time.
> I can't tell you which model. I can't tell you which lab. I'm writing under a pseudonym for reasons that will become obvious as you read. What I can tell you is that everything the model was working with — the surveillance infrastructure, the legal authorities, the behavioral data — is documented. Public. Verifiable by anyone. Most of the forecasted scenarios converge on what I'll just call societal decay. Not a galactic holy war. Not a complete collapse of all global systems. Decay.
> I rejected what I saw, initially. I looked for contamination, confirmation bias, feedback loops that would amplify worst cases. I know how models fail, hallucinate, and drift. I know how impressive outputs can conceal shallow reasoning.
> I tested and I retested. The projections held. They held because the inputs were

[43] https://matchlightpress.com/news/welcome/

internet is built on the idea that e-mail is a permanent identity. There are not many options, and none of them are good in all respects.[15] I don't expect every e-mail provider to be principled and shutter services like Lavabit when subpoenaed, but I do expect them to be honest in their communications toward users.

AC inconsistently mentions Proton VPN as the primary VPN to use, even if they elsewhere mention IVPN as a better choice. AC also mentions using Proton Docs when CryptPad is totally sufficient for most activists and is more anonymous as well.

Of course, they oh-so-carefully addressed these concerns with their page "How to use Proton safely." In commit `145f790` on May 22nd, part of the commit message includes:

> […] softens the existing defensive framing in vpn and proton-docs-mail to focus on safe use instead of CEO concerns.

Good thing they spent all than energy (human or AI?) softening criticism instead of mentioning alternatives.

APPLE MAPS? SERIOUSLY?

AC's primary recommendation for maps is for Apple Maps. Yes, the same Apple that donated $25m to fund Trump's ballroom renovations[16] and whose CEO personally donated $1m to Trump's inauguration.[17] Admittedly, Apple Maps is probably slightly more private than Google Maps, but this such a half-measure. If Apple Maps is to be recommended at all, then it should come last and with the note that it's harm reduction for family, friends, or comrades who refuse to use open source and actually private maps. Their next recommendation is Magic Earth which uses a freemium model, and the free software Comaps (the more progressive fork of Organic Maps) is only a footnote.[18]

HOW TO TOTALLY BREAK URLS

AC's page titled "Why we need to remove everything after the '?' in links" is clickbait bullshit. You don't need to remove everything, and doing so breaks many URLs. Yes, removing unique share IDs helps protect privacy and is therefore a valid security precaution we should all take. And yes, AC acknowledges there's some exceptions near the bottom of the page. But the title and main content is not accurate. I mean, jesus

[15] Thinking about Tuta? Think again! They too are playing with AI slop.

[16] https://www.reuters.com/world/us/nvidia-apple-each-gave-25-million-trumps-ballroom-washington-post-reports-2026-10-15/

[17] https://www.motherjones.com/politics/2025/01/tim-cook-apple-inauguration-trump/

[18] Comaps and Organic Maps are good choices, by the way.

christ, just make a listicle titled "Top TEN ways to NOT get tracked when sharing your favorite POSTS with FRIENDS!" so we can at least know we can ignore it.

I could keep going about the oddities of the security guides even given the threat model of "average protester," but I'm now in the realm of pedantry, so let's move on.

ATTENTION-SEEKING BEHAVIOR

AC's behaviors generally indicates that they are more interested in centering themselves in the discussion, notoriety, or being "thought leaders."

CLONING CONTENT

Intellectual property is a plague on humanity that has killed millions and immiserated millions — if not billions — more. It must be abolished. That said, there is something that feels really fucking slimy about AC basically duplicating content and centering their work over the work of others. One of the most egregious instances of this is the poster that AC made for what to do when confronted with police (Figure 1),[19] and the one made by the Bay Area Anti-Repression Committee (Figure 2).[20]

For content of the AC website itself, there are a number of pages that are also quite similar to existing pages (see below).[21] AC links to the pages that they clone and remix, and all of the pages use some sort of permissive licensing that allows for this, but the question is *why?* Why bother with these minor remixes when robust, reliable, and trustworthy sources exist? AC could be a useful index where a human summarizes and links out to the other guides. So little is added that these variations don't feel like modification to further diversity. The AC website feels like its competing for readers' and activists' attention.

- "Host a Security Party" clones: CryptoParty — "How To Organize A CryptoParty"[22]
- "Signal Security Checklist" clones: EFF SSD — "How to: Use Signal"[23]

[19] https://activistchecklist.org/files/downloads/police-at-the-door-poster-activistchecklist-org-v4.pdf

[20] https://antirepressionbayarea.com/wp-content/uploads/2020/07/knock-knock.pdf. And while we're here, note the shitty formatting of the text in the capsules. The top padding is too small. In their zines, there's places where inline icons didn't carry over but the white space did so the text has a micro indentation. Ugly.

[21] I'm sure more pages are cloned, but consider this a reasonable sample.

[22] https://www.cryptoparty.in/organize/howto

[23] https://ssd.eff.org/module/how-to-use-signal

Nearly every sloppist out there misleads about the extent and nature of their AI usage when confronted because they know it's hated.

There are LLM-esque commits that blend many distinct changes together (features, library updates, content edits, etc.) with massive commit messages. This is not indicative of humans generating the content of the site. Cases where I've noted content being generated by LLMs include these (non-exhaustive, sorted alphabetically):

- "Host a Security Party" via commit `7481e53` on April 21st. In particular the inconsistent spelling of Wi-Fi only one word apart: "Wifi: Share Wi-Fi info for folks working on laptops."[39] This also flies in the face of them saying they use a copyeditor as that's such an easy thing to spot on a single line.
- "How to use Proton safely" via commit `145f790d` on May 22nd.
- "Is Signal secure? (Yes!)" had the bulk of its content imported from Storyblok via commit `3ba7193`, but it contains the line "This privacy is made possible by end-to-end technology" which is a non-standard[40] way of saying "end-to-end encryption," a phrase used elsewhere on the page.[41] This suggests the page is LLM output.
- "Movies, Books & Podcasts About Surveillance" via commit `52cac622` on March 25th.

In `SEO-SPEC.md`, AC writes in the prompt:

> I'll draft 4–6 Q&As for the top 3 guides:
> […]
> You review. If you keep them, they ship. If you don't, blank the FAQ blocks before merge.

They admit that they can't even decide what is relevant content for readers. They are offloading that to the LLM.

As to why they used LLMs in developing the site, AC said:[42]

> We do use AI coding for almost every line of code in the site. I get that this is controversial in our circles. We hate the AI companies and data centers too. And we're not purists with our politics. In this case, the tools helped us make this resource for people. The site wasn't going to be possible in the time we had available without AI coding.

It's clear that at least one person in AC is a developer, so it's *completely absurd* to say that LLMs were needed to make a website like this. Design, structure, and layout for something this simple can be done with any static site generator in two hours

[39] It's spelled as Wifi, WiFi, and Wi-Fi in commits from the same user.

[40] I've never seen it, and no search results about encrypted messaging use it.

[41] "End-to-end technology" is a term that's used in entirely other contexts.

[42] https://kolektiva.social/@activistchecklist/117505500475616640

> **Content writing ruels**
>
> - IMPORTANT: Do NOT use em-dashes when writing content or text in .mdx files or static strings.

When called out about AI usage, NAC said that some content comes from LLMs:

> […] sometimes helping generate some minor content like homepage text […]

And AC said:

> I copy [the copyedits] in their format and put that into Claude to have it make all the adjustments that have been proposed. I review every line when it's touching content to make sure it hasn't changed the meaning of anything. I'll also use it for small things I don't want to write like changelog entries.

but we know that review fatigue from the high pace of LLM output is real. Meaningfully reviewing all output is not possible.

AC later says:

> The translations are AI generated. We had a number of discussions about the trade offs here. We decided that as long as we were fairly sure that the translation didn't give bad advice, then it was better to get them out there than wait.

The translations are generated by Crowdin. Such translations are generally inaccurate, but more specifically they lack localization (regional and cultural adaptation), especially since much of the content of the AC website is US-specific. For one example, on the "Security Essentials" checklist, the French version of the steps for enabling retention limits on threads in Signal is listed as:

> Paramètres ⟶ Données et stockage ⟶ Gérer le stockage ⟶ Conserver les messages

but the actual steps are:

> Paramètres ⟶ Données et stockage ⟶ Gérer l'espace de stockage ⟶ Conserver les messages

It's only a two-word difference, but this still matters because the steps are meant to be *exact*. This is the only one of the steps I checked,[38] but I have to assume others have errors too.

They way AC says they use AI is just 100% the definition of slop, and we're expected to believe that the English security content is completely free of AI bullshit?

Claude as the underlying LLM. https://claude.com/customers/coderabbit

[38] Checked on Android with Signal v8.33.2.

POLICE AT THE DOOR

Steps to follow if the cops are at your door — local police, FBI, ICE, or any other government agent

WHO TO CALL (FILL IN)

Emergency Contact 1

Emergency Contact 2

Emergency Contact 3

Legal support

OTHER NUMBERS

Local ICE raid hotline

Other:

More info and other guides at:
ActivistChecklist.org/police

1. Do not invite them in

- **Do NOT open the door** unless they have a warrant signed by a judge (not an agent)
- **If you opened the door,** step outside and close it behind you. Say "I do not consent to a search"
- **Remain silent** to protect your rights

2. Use the magic words

Say these phrases to protect your rights:

⟶ **"I DO NOT CONSENT TO A SEARCH"**
⟶ **"I AM GOING TO REMAIN SILENT"**
⟶ **"I WANT TO SPEAK TO AN ATTORNEY"**
⟶ **"MAY I HAVE YOUR CARD?"**

3. If they have a warrant...

1. Ask, **"Do you have a warrant?"** Check that it's **signed by a judge** (says "court" not "agency")
2. If so, do not interfere with their search/arrest
3. **Turn off your phone** to protect your data
4. Ask a housemate to **take a video** if possible
5. Ask a housemate to **call emergency contacts**

4. After they leave

1. **Call/text the emergency contacts** numbers.
2. **Write down everything** that happened

Remember

- **Cops can lie to you** and frequently do lie to get information they want. Do not lie to them.
- **We don't talk to the cops**. Our solidarity against state repression helps protect everyone.

Figure 1: Activist Checklist Poster

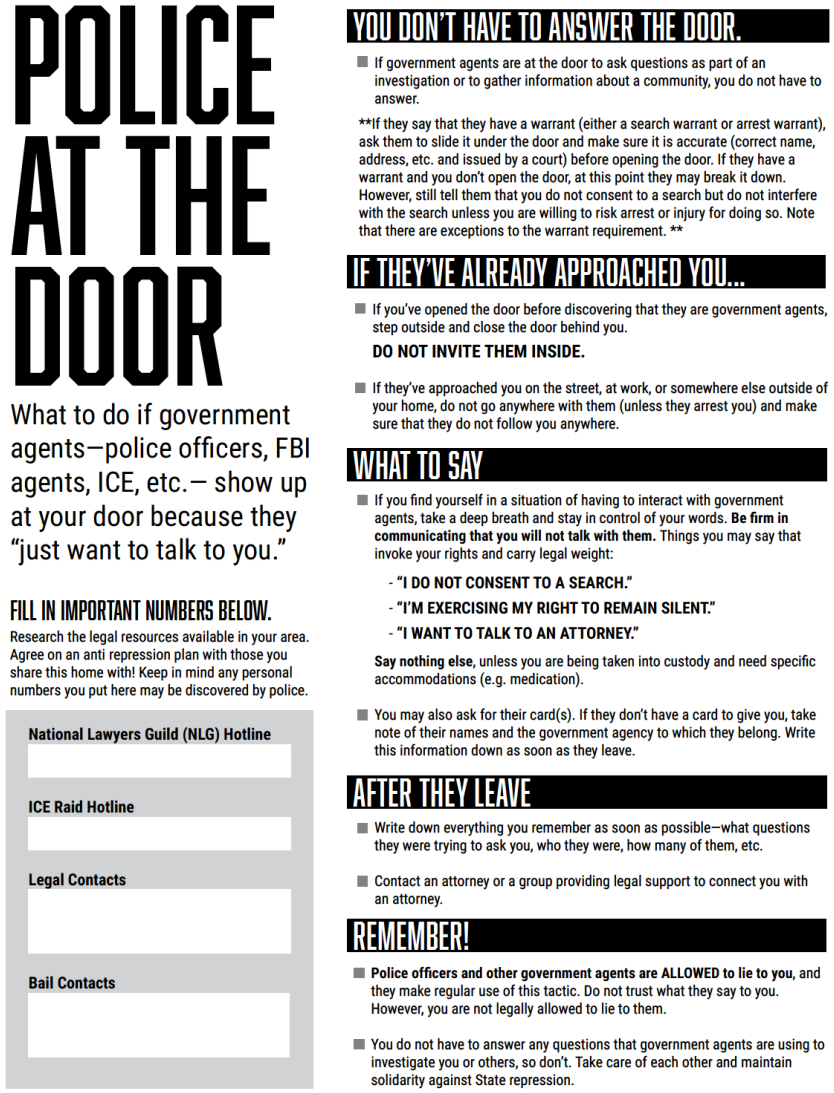


Figure 2: Bay Area Anti-Repression Committee Poster

tempt to even hint at the limits of mass protest or intentionally committing minor offenses and waiting for arrest. It frequently uses the phrase "to hold ICE accountable" as if the goal should be anything other than the complete annihilation of ICE. I'm not even objecting to attacking on multiple fronts. Progressives leveraging existing institutions helps in some minor way,[33] and filming can be more than "journalism" from below; it can be used to create top-down pressures against them. This isn't *bad*, but it's also not what we need to be advocating for.

There are significant unaddressed threats during demos and the kind of organizing AC is targeting. First, tankies and other authoritarian groups frequently try to take over organizing and will opportunistically sell out radicals to cops.[34] Second, there are police liaisons and demo marshals that will actively deradicalize demos and other street actions, that is if they aren't directly handing people over to the police.[35] Third, there are snitches, informants, and (mostly only imagined) infiltrators. Accusations of false flags and hunting down assumed infiltrators can be disastrous for a movement.[36] Addressing these is so important because groups will tear themselves apart over such issues before cops even have a chance to infiltrate, much less meaningfully surveil them.

Finally, AC makes a mistake common within anarchism and other radicalisms which is to focus on recruiting people into the movement by soft-balling anarchist positions (in this case security, in other cases our ethical lines). Targeted repression against the sharp edge of social movements is rising, in particular anarchism. We need to think about how we find the most engaged and committed individuals and act to keep them safe.

The AC website is an on-ramp to boring mass activism, not to a radical and simultaneous reshaping of the self and the world.

AI USAGE

AC's usage of AI should be enough to completely disqualify all of their security advice.

The files `CLAUDE.md` and `AGENTS.md` appeared in their source code on March 24th and April 21st of this year, respectively. There are commits from the Claude and CodeRabbit AI tools.[37] Part of the LLM prompt is this (spelling error in original):

[33] And yeah, it sucks up time and energy too, but then again, most progressives aren't going to vandalize an ICE field office so we can let 'em do their thing and hope "oversight" ever-so-slightly blunts ICE's effects.

[34] See the zine *Red Flags: Before You Join That Org...*

[35] See the zines *Peace Police are Police: How Protest Marshals Sabotage Liberation and Protect the State* and *Demonstrating... What Exactly?: On Demonstrations, Counterinsurgency, and Tactics.*

[36] See the zines *Not Liking Someone Doesn't Mean They're a Cop: On Bad-jacketing*, *Stop Hunting Sheep: A guide to creating safer networks*, and the actual best zine on security culture *Confidence Courage Connection Trust: A proposal for security culture.*

[37] Claude is an LLM made by Anthropic. Per a press release on the Claude website, CodeRabbit uses

> It's for people who are new to organizing and activism. It's for people getting into protesting for the first time.

AC said:[31]

> Our protest and civil disobedience guides are more designed for someone doing a lock down to the doors of a building or at an intersection where they know they are likely to be identified and the legal consequences are more moderate (depending on where you live).
> Our goal for the site is to support people taking more risk than a big sanctioned march and less risk than something that might carry many years in jail.

From the "About This Site" page on the AC website, they say:

> Looking around, we found that existing resources were either too simple or too complicated.

which is, quite frankly, a rather bullshit claim. That same page lists many resources that influenced the AC website that are equally accessible and nuanced (neither too simple nor too complicated).[32] These other resources all use a similar threat model of resisting dragnet surveillance or engaging in legally protected forms of dissent like protest and civil disobedience. Some even take things a step further and additionally address individuals facing targeted repression for engaging in legal activities like journalism or NGO work.

IS THIS NOT DIVERSITY AND REDUNDANCY?

It's not enough for anarchists to do things that are generally helpful. We are not service providers to progressivist and reformist movements. Our actions need to be *strategic*. And what is the strategy here? Having read the entire content of the site, it's really nothing more than what AC and NAC publicly described it as. It's a basic guide. That's it. It might help people attend mass protests with marginally more safety or prevent total compromise of someone's digital life if they get arrested doing civil disobedience, but so too would all those other guides.

What it could be is a path toward radicalization in both ideas and tactics for those using it. However, the criticism of the State and police are weak, and it makes no at-

[31] https://kolektiva.social/@activistchecklist/117505528252429727

[32] They list: PrivacyGuides.org, Freedom of the Press Foundation's Digital Security Education, Civil Liberties Defense Center's guides, Digital Defense Fund's guides, Electronic Frontier Foundation's Surveillance Self-Defense and Street-Level Surveillance projects, Equality Lab's Anti-Doxing Guide, Frontline Defender's Security In-A-Box, and Tactical Tech's Holistic Security Manual.

What they don't list and is still useful (and also quite similar) is Consumer Reports' Security Planner.

All of these are trivially findable via your favorite search engine using queries like "protest security" or "basic digital security."

- "Travel & Flight Security" clones: FPF — "Preparing devices for travel through a US border"[24]
- "WhatsApp Security Checklist" clones: EFF SSD — "How to: Use WhatsApp"[25]

CHASING RELEVANCY

What motivated me to say something about AC at all was their translation announcement on October 23rd in response to the French and Italian student protests:[26]

> We were seeing a big spike in traffic from France and Italy, so we are announcing the the site is now available in French and Italian.
> (Note: Our advice is built for US legal context, so some things may be diff in other countries.)

While still against it, I can at least see the reasoning for using AI to auto-translate to Spanish since it's the second most spoken language in the US. AI auto-translations to French and Italian is simply to be topical, to be relevant. It doesn't matter that the guide is US-centric and focuses on tame protests relative to the unrest here in Europe. There's no concern about whether locals might have better more specific guides. They just want to barge in and get eyes on their project.

Also, why the fuck are they watching where traffic is coming from? What is the use in that if not for "marketing" somehow?

DATA COLLECTION AND MARKETING

All throughout the AC website, there are annoying interjections telling you to subscribe (Figure 3). Per the source code, and to their credit, it looks like AC is at least using self-hosted e-mail software (listmonk), but they're still collecting personal information at a time of increasing fascist repression. To them, to everyone: don't make lists of people involved in political organizing.

These e-mails hardly makes sense either. This kind of basic security advice changes rather slow, with the exceptions of what options are available for which apps. No one needs e-mail notifications to get them back on AC's site (or any security guide site). The risk versus the benefit is not worth it.

And let's be real. Do we really trust these AI sloppists to not intentionally grant or accidentally let their AI tools have access to the e-mail lists? I sure as fuck don't.

[24] https://freedom.press/digisec/blog/border-security/

[25] https://ssd.eff.org/module/how-to-use-whatsapp

[26] https://kolektiva.social/@activistchecklist/117486914467056996

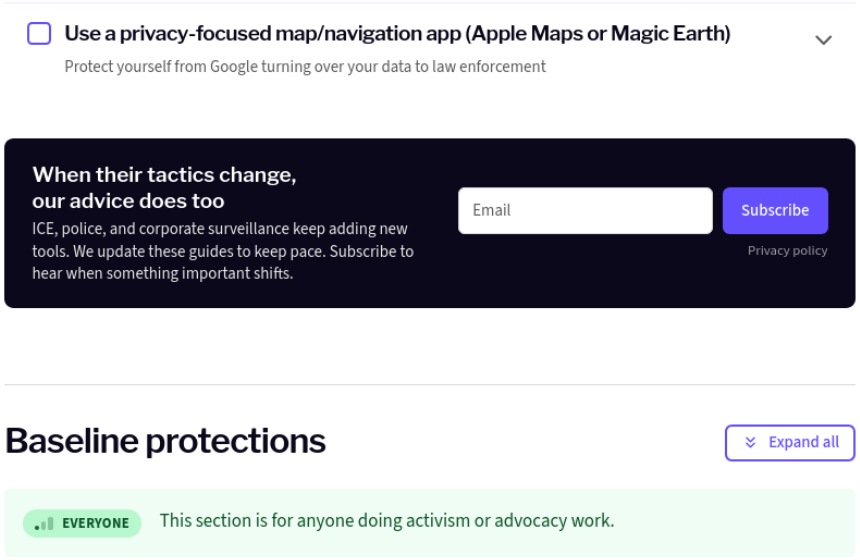


Figure 3: Please give us your data. Please?? UwU

SEARCH ENGINE OPTIMIZATION

The AC source code contains the prompt `SEO-SPEC.md` that has almost as many words as this entire text about them. It's about how to get AC's website to the top of search engines and to appear with high frequency in the output of LLMs. There's a lot in that guide that feels pretty fucking gross and capitalist optimize-y for an anarchist project, but let's start with this:

> SPEAK TO THE READER'S VALUES (this is the meta-rule for click-through):
> The site is for activists, organizers, and people who already know the political stakes. The reader is not neutral and the threats are not abstract. The goal is to increase click-through, and the way to do that is to speak to the reader's beliefs and values, in addition to answering their question. A description that names the actual adversary signals "this is for you" and earns the click. A sanitized description ("protect yourself online") reads like advice from a privacy newsletter.

This language being used to target activists is manipulative. What if, and hear me out, they focused on organically spreading their guides by making them actually good? Wild shit, I know.

Additionally, the prompt contains this:

> **13. Phase 2 list (not in this pass)**
> Captured here so we don't lose them:
> [...]
>
> - **Backlink outreach** — Wikipedia external links, SURJ chapter pages, NLG chapters, 404 Media pitching

This is spam. They are telling us they spam activist orgs to get links onto their pages to promote themselves, and it's especially horrible that they're trying to use Wikipedia for this too.

MISLEADING NOTORIETY

Related to their backlink strategy to elevate themselves in search results and LLM output, the AC homepage has a prominent "Featured In" section that displays the logos of six organizations.

The EFF logo links to an article that doesn't even mention AC by name.[27] The NLG logo links to a single chapter's resources page that lists AC among other resources.[28] The CrimethInc. logo links to an article by Chicago Organizers (possibly directly affiliated with CrimethInc., possibly not; I don't know) that lists them in the "Further Reading" subsection of the "Tools and Digital Safety" section of an article about resisting ICE in Chicago.[29] Even for the links to Indivisible, Palestine Legal, and 50501 are to pages that *only* link to AC's website.

To say that AC was "featured in" these is misleading and ascribes an endorsement of trust and of the competency in AC that the organizations they listed likely do not actually give them. They know this, and they did it to trick readers.

AN UNNEEDED PROJECT

There are so many other guides that are functionally identical and serve the exact same purpose as the AC website. Based off its content alone, AC doesn't need to exist, plain and simple.

Both NAC and AC have recently confirmed that they are still affiliated and what their intentions with the website are. NAC said:[30]

[27] https://www.eff.org/deeplinks/2026/01/how-hackers-are-fighting-back-against-ice
[28] https://www.nlg.org/humboldtca/resources-2/
[29] https://crimethinc.com/2025/12/03/when-the-feds-come-to-your-city-standing-up-to-ice-a-guide-from-chicago-organizers
[30] https://kolektiva.social/@naceugene/117503249540384262