



THE NEW INQUIRY

<http://thenewinquiry.com/features/security-culture-is-good/>

(<http://thenewinquiry.com/>)

Organize and resist with the TNI 2017 calendar: <https://t.co/tH1jV5GT10>
(<https://t.co/tH1jV5GT10>) <https://t.co/5XvocWhmfX> (<https://t.co/5XvocWhmfX>)
(<https://twitter.com/thenewinquiry>)

SEARCH

ESSAYS & REVIEWS (/ESSAYS)

FEATURES
(/FEATURES)

BLOGS (/BLOGS)

&, MEANWHILE (/AND-MEANWHILE)

NEWS (/NEWS)

MAGAZINE (/PUBLICATIONS/MAGAZINES)

ARCHIVE (/PUBLICATIONS/MAGAZINES/#LISTING)

THE NEW INQUIRY NEEDS YOUR HELP

(<http://thenewinquiry.com/support-tni-2017/>)

Security Culture Is Good

By KADE CROCKFORD ([HTTP://THENEWINQUIRY.COM/AUTHOR/KADE-CROCKFORD/](http://thenewinquiry.com/author/ka-de-crockford/))



Take these precautions to protect yourself and your loved ones from the state

Five easy things you can do right now, and some basic tips:

Start simple. These are bare-minimum security requirements for anyone using modern communications tools.

December 19, 2016

DOWNLOAD
PDF



(<http://thenewinquiry.com/wp-content/uploads/2016/12/57securitycultureis>

- Download HTTPS Everywhere and Privacy Badger for your browser.
- Turn on two-factor authentication for all your social media and email accounts.
- Update all of your software as soon as new versions become available on your phone and computer (including your browser). Turn on automatic updates.
- Fix your passwords! Use a password manager to keep track of them.
- Encrypt your hard drive and your smartphone.

For more detailed information about how to do all of these things, and which encryption and password manager software you should trust, visit: libraryfreedomproject.org (<http://libraryfreedomproject.org>).

Also, keep in mind that deleting tweets and using an “Incognito” browser window won’t do shit to stop you from being monitored. The Internet is forever.

If you’re editing documents as a group and don’t want to use Google docs, try a Riseup pad (<https://pad.riseup.net/>). Sandstorm (<https://sandstorm.io/>) is another alternative that has some cool features.

Finally, watch out for common social engineering tricks. If someone sends you an email that looks weird, don’t click on the link or attachment. If your friend sends you a link that looks weird, call or text them to make sure they actually sent it. The most common way people get owned online is through social engineering. It can be tricky to avoid if you’ve got a persistent and powerful adversary like the NSA, but common sense and paying careful attention to what you click will protect most people most of the time.

Encryption: Use it, but be aware of its limitations.

You probably know by now that end-to-end encryption is our best defense against dragnet government and corporate surveillance. “Use Signal. Use Tor” is a joke at this point in the security community. It has become a joke because it’s a cliché; it’s a cliché because it’s the best advice for people looking to easily protect themselves online. But neither of these tools is foolproof, meaning they won’t necessarily stop the cops or FBI from spying on you. Nonetheless, you should use them religiously—if you can.

Signal is a free, open-source app that encrypts voice-over-IP calls and text messages. It works well and it’s easy to use, as long as your communication partner also has the app installed. Signal is great because it doesn’t only protect the content of your communications—it also protects associational metadata. That means if cops send a warrant or court order to Whisper Systems (the company that runs Signal) asking for information about who you’ve been calling and texting through their app, they won’t get anything in

return. The company doesn't create or keep these records. Since Signal allows group chats, it can work as a replacement for email (which is notoriously insecure) if you need to keep information private. This is important for organizers and you should make use of this feature.

Tor is a browser that protects your Internet activity from the spying eyes of Comcast, Time Warner, and the FBI alike. Using Tor won't encrypt the content of your Gmail, or keep Facebook from tracking your thoughts and associations. But it will make it more difficult for companies and governments to track everything you do online.

The trick with these two security tools is that **they only work if you use them**, and they have limitations. Primary among those limitations is the threat of hacking. If someone installs malware on your device (on either your phone or your computer), no amount of encryption is going to stop them from reading everything on it. Encryption protects data in transit and at rest, not on your (unlocked or hacked) machine. In other words: if someone has your password, or installs malware on your device, Signal and Tor are helpless to stop them from owning your digital life.

Furthermore, Signal only works if you have a data connection or wifi, making it a crappy option for people who rely on SMS and phone calls to communicate. It also doesn't run on Windows phones. Despite these limitations, it's our best option for easy-to-use, secure, free communications technology—that is, besides whispering in the woods. Use it to tell your weed dealer how much dank you want, to tell your comrades where to meet up, and to tell your mom you love her. Use it for everything.

Threat modeling: Do it.

The concept of threat modeling is relatively simple: perform an analysis of your unique situation to protect yourself from harm. Ask and answer the following questions:

- What information are you trying to protect?
- Whom are you trying to protect it from?
- What are the capabilities of your adversary?
- How can you protect information from your adversary, given its capabilities and your own?

Let's consider a possible scenario:

You're an organizer in New York City. You're planning a direct action where you and some comrades will lock down at a bank in Brooklyn. You want to keep the existence of the direct action and the identities of the people organizing it secret from the NYPD and the bank's security team.

The NYPD—your adversary—has advanced surveillance capabilities. You don't know much about the bank's security team, but you do some research and find out they've got security officials working alongside the NYPD at the Lower Manhattan Security Initiative. Given the department's penchant for obsessive secrecy and its love of surveillance, it's probably got a lot of toys and powers that you don't know about. It's not quite the NSA, but for a police department it's as close as they come. The NYPD has cameras all over the

city, and access to the MTA's surveillance feeds. The department has cellphone-tracking stingrays, perfect for spy cops who don't want to bother with courts, warrants, or the limited outside oversight they provide. NYC's police also have an obsession with crushing dissent, and an enormous budget with which to do it. They might also use undercover informants or police operatives in leftist movements in the city, but you're not totally sure.

In order to protect yourself and your crew in this hostile environment, you may want to take the following approach:

- Trust your comrades. This is really important. Technology can't stop human beings from fucking up or becoming disloyal. That means you shouldn't organize direct actions with people you don't know or trust, and you shouldn't announce that you're planning a direct action or invite people to join you unless you know them, or know and trust someone who can vouch for them. Some people might call this paranoid, but trust is the foundation of security.

- Make sure that everyone involved in the action is on the same page when it comes to security. You don't want people getting smacked with conspiracy charges, so this is important for all of you—not just the handful of people who are locking down. Come to a security agreement before you get into details about what the action will look like and how it will work, and before you agree to roles. Devise a threat model together as a group, and stick to the agreements you make. For example, you may want an agreement from everyone involved that you'll only use Signal to communicate, that you won't discuss the action outside the circle of its organizers, and that you won't put any information about the action in any digital format the group hasn't approved of collectively. Finally, go over the basics of what happens if and when you're confronted by law enforcement. Most important, as always, is to keep your mouth shut. You might think you're being clever by telling the police something false or giving them only limited information to throw them off track, but you're not being clever. **Do not speak to the police or the Feds.** Make sure everyone in your group understands that at the outset. If necessary, do some role-playing to drive the point home.

- Prior to the action, make sure everyone in your organizing crew deletes all of their Signal messages. To do this, go to settings > privacy > clear history logs. A screen will appear asking if you're sure you want to do this. Press the red "I'm sure" button. That way, if someone in your group is arrested, the cops won't be able to read the entire organizing thread if they illegally search the phone or obtain a warrant to legally search it. This is an important self-defense measure to counter possible conspiracy charges.

- Don't discuss the action on Facebook (or, depending on the group agreement, Google products). Treat Facebook like it is not private—even the messages part. We aren't totally sure right now whether the NSA can crack Facebook's encryption, but we know the agency hoovers up Internet traffic with a gigantic vacuum and has installed employees in tech firms working undercover to steal their secrets and compromise their products' security. We also know that the FBI has access to a lot of the info the NSA steals. Therefore you should consider Facebook, like email, presumptively

available to the cops. If you don't want them reading it, don't put it on that godforsaken website. The same goes for Twitter.

- If you're planning something public to go along with the direct action, keep the planning of the two actions separate. Choose a liaison among your direct action group who can attend meetings to help plan the larger public action, so your group is in the loop—but don't tell people at the public meetings that a secret action is underworks. Don't worry about being perceived as some kind of revolutionary vanguard. You aren't keeping the direct action secret because you think you're cool; you're doing it because you want the action to happen, and you don't want all of your comrades going to jail. Security isn't about glamour, it's about solidarity.

- Don't meet to discuss the action in public places where people might overhear you. You never know who's a narc, an undercover cop, or even a right-wing blogger. You also may want to avoid leftist organizing spaces. If I were an FBI agent I'd have bugged those spots a long time ago.

- Finally, always keep in mind that the state will likely be extra vicious with your Muslim, Black, Latino, Arab, POC, immigrant, trans, and queer comrades. When you're planning an action, think about how to leverage existing privilege to forward the group's goals, and make sure you protect the members of your group who are most vulnerable to state oppression. While an arrest might not be such a big deal for a white cisgendered U.S. citizen with access to money and a flexible job, it could mean deportation for an undocumented comrade. As the saying goes: "Be careful with each other so you can be dangerous together."

Now, this "locking down in a Brooklyn bank" activist scenario is very different from another one folks need to grapple with: you're a Muslim dad in Wisconsin, and you just want to go about your life without worrying that the FBI will force you to become an informant or try to entrap your teenager into an "ISIS plot." The next section provides the most important information for a person dealing with this type of threat.

What to do if the FBI comes for you:

Over the decades, the FBI has developed a very efficient means of screwing people over: getting them to talk to its agents. If FBI officials contact you at home or at your office, asking to have a chat, take their business card and inform them that your lawyer will be in touch. Politely decline any other conversation with the agents. This is extremely important. You should never talk to the FBI without your lawyer present, even if you think you have "nothing to hide" or you want to help them. You must help yourself first. And the only way to do that is to keep your mouth shut.

When the FBI interviews someone, they send two agents: one person asks questions, and the other takes notes. The stenographer then goes back to the office and types up the notes into an official document known as Form 302. This is the government's official record of the interview, and it can and likely will be used against the interview subject. If an FBI official writes on the 302 that you said you were at a basketball game Sunday morning at 11, and then you later tell a grand jury that you were at the basketball game at 10, you can be charged with lying to a federal agent. A conviction for lying to a federal agent will land you in federal prison for years. This is how the FBI puts people in a vice, and gets them to inform. The truth doesn't matter; the only thing that matters is what's written on that Form 302.

This is why it's absolutely critical that you do not speak to the FBI under any circumstances without your lawyer present.

In many (if not most) cases, when your lawyer follows up with agents to schedule the interview, the agents will drop it. It's more difficult for them to manipulate people who know their rights. Don't be fooled by their nice smiles or their vague threats—"We can do this the hard way, or we can do it the easy way now..." or "This could be bad for you if you don't talk. It makes it seem like you've got something to hide."

If you're reading this and you're worried that perhaps an elder or someone else in your family or community doesn't know not to trust the FBI, read up about how the FBI does this to people, and educate them. (Go to privacysos.org (<http://privacysos.org>) and search for "FBI manipulation" for some stories; show them the films *The Newburgh Sting* and *(T)ERROR*.) People want to help, they don't want to be seen as obstructing justice, and they want to believe the government will protect them. But the unfortunate reality is that the FBI cannot be trusted and justice isn't usually what they seek—especially when it comes to Muslims and dissidents.

Finally, beware of people who are new to the community and offer money or power to the disenfranchised, destitute, or intellectually disabled. The FBI has more informants on its payroll today than it did at the height of the COINTELPRO era, and they are hard at work every day trying to convince misguided or lost young people to get involved in illegal activity, sometimes for promises of money, other times for promises of heavenly rewards. Study the way the FBI has manipulated people using informants, and then educate your community. Like a predator attacking a herd of deer, the FBI goes after the weakest people in communities—those who for whatever reason cannot defend themselves. Keep that in mind and do whatever you can to protect those people.

Know your rights. And flex them!

Disclaimer: This is not legal advice. If you want legal advice, call a lawyer.

Knowing your rights can mean the difference between you getting locked up and you walking away from the cops to go home. You've got to know your rights in order to flex them. Here are some important ones:

• You have the right to remain silent, and **you must exercise that right**. It's the best defense against getting arrested, charged, or convicted for some bullshit. These are **the only things** you should say to the police:

- "Am I being detained? Am I free to go?"
- "I do not consent to this search."
- "I want to talk to my lawyer."

• If the police ask you, "Is this your computer?" or "Is this your phone?" **don't answer them**. See above for the only three things you should ever say to the police without your lawyer present. Simply say: "I want to talk to my lawyer."

• Government agents must obtain a warrant to search your cell phone, even if it is seized during your arrest. They cannot search your phone simply because they arrested you; they need separate probable cause to get into your phone. If cops demand that you give them your phone password, tell them you want to speak with your lawyer. Do not give them your password until you've gotten the ok from your attorney.

• Important: Don't use the fingerprint feature on your phone as your password. For arcane legal reasons it may provide less protection than a password.

• Unless you're driving, you are not required to show police your ID in many states; in others, you can be required to show ID to an officer if she has "reasonable suspicion" to believe you're involved in criminal activity. Nowhere are you required to show ID to a cop if they don't have "reasonable suspicion."

• If you're stopped on the street or at a protest and a cop asks for your ID, ask, "Am I being detained or am I free to go?" If you're free to go, calmly walk away. If you are being detained, ask why.

• **Make sure you look up the law in your state.** If you cannot be arrested for refusing to show your ID, don't produce it. If you can be arrested for refusing to show your ID, consider that before you act. If you aren't sure how to do the research to find out what your state law says about whether you are required to show an ID when she has "reasonable suspicion," try calling the state affiliate of the ACLU to see if someone there can help you.

• Keep in mind that lots of cops don't care about the law and will arrest you simply for disobeying them. Just because the charges won't stick doesn't mean you want to go to jail over some bullshit like refusing to give a cop your ID. Know your own ability to take risks, and know the police department in question. If you don't think the cop will freak out and arrest you because you disobeyed him, assert your rights. If you think he might, and you've got a kid at home and can't risk arrest, you might want to make a different choice. Know yourself, your adversary, and your limits.

How serious is all of this? It's serious as fuck, actually.

(<http://thenewinquiry.com/publications/magazine>) Resist the urge to take lightly the advice I've dished out above. It might seem like a lot of these measures are evidence of unjustifiable paranoia, but with organizing as with sex, safety comes first. And just like contraception can't stop 100% of pregnancies, there's no way to eradicate the possibility that you'll get bagged. That doesn't mean you shouldn't wear a condom, or take care to protect yourself and your comrades from state repression. It would be foolish not to.

In Obama's America, Black Lives Matter organizer Jasmine Richards was convicted




(https://www.democracynow.org/2016/6/2/black_lives_matter_activist_convicted_of_felony_lynching) for de-arresting a comrade at a demonstration. Richards faces four years in prison. This was in California, not Mississippi. Cops across the country—in addition to the FBI and DHS—have used military style tactics and surveillance equipment to undermine opposition to the carceral/police state. The FBI has spent the past 15 years treating Muslims like the new communists—an “enemy within.” Obama deported more undocumented people than any prior president in U.S. history. Meanwhile, the state's centuries-old war on Black America rages on. In Trump's America, do you think the state's repressive apparatus is going to stop engaging in this behavior, or ramp it up?

No matter who you are or what you look like, you must take responsibility for protecting yourself and your community from state harm. This isn't a game. People's lives and freedom are on the line. The ability of our movements to push back against the rising tide of fascism will depend on our ability to organize coherent resistance. Keep yourself and your comrades safe. And good luck out there.

Previously by

KADE CROCKFORD

([HTTP://THENEWINQUIRY.COM/AUTHOR/KADE-CROCKFORD/](http://thenewinquiry.com/author/KADE-CROCKFORD/))

 (<https://www.facebook.com/sharer.php?u=https%3A%2F%2Fthenewinquiry.com%2Ffeatures%2Fsecurity-culture-is-good%2F>)  (<https://twitter.com/share?url=https%3A%2F%2Fthenewinquiry.com%2Ffeatures%2Fsecurity-culture-is-good%2F>)  (<http://www.tumblr.com/share>)

SUBMIT (/SUBMIT-TO-TNI/)

TERMS OF USE (/TERMS-OF-USE/)

**CONTACT US (/CONTACT-US/)
SUPPORT TNI (/SUPPORT-TNI/)**

DESIGNED BY IMP KERR (/IMPKERR.COM/)

BUILT BY KRATE (/WWW.KRATEDESIGN.COM/)