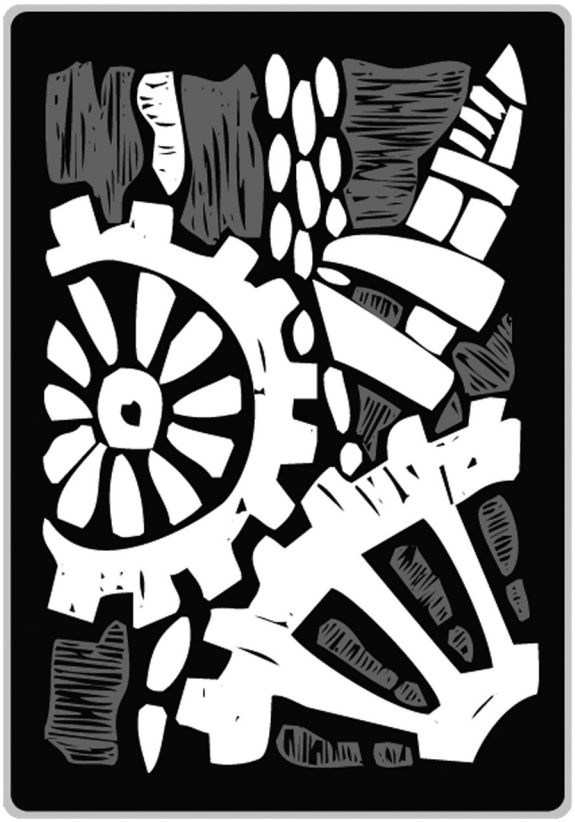
SECURITY CULTURE FOR ACTIVISTS

brought to you by:

THE
RUCKUS SOCIETY
Actions Speak Louder Than Words



SECURITY CULTURE for ACTIVISTS

The Ruckus Society provides environmental, human rights, and social justice organizers with the tools, training, and support needed to achieve their goals, through the strategic use of creative nonviolent direct action.

Visit **www.ruckus.org** for more online tools and resources, direct action community news, upcoming training opportunities, or to request training or action support for your group.

A resource by The Ruckus Society, written by Jessica Bell and Dan Spalding

Design: Jake Conroy / TwelveTwentyone.org

TABLE of CONTENTS

WHAT IS SECURITY CULTURE?

A security culture is a set of customs and measures shared by a community whose members may engage in sensitive or illegal activities. Security culture practices minimize the risks of members getting arrested or their actions being foiled.

In other words, while we are trying to stop bad things from happening, our powerful opponents (usually governments or corporations) are working hard to stop us. This guide is about the security measures activists can take to protect ourselves and make our work more effective.

What do our opponents do to stop us?

This guide mostly focuses on the actions of law enforcement, such as intelligence officers and police, as it usually has the greatest authority to target activists.

1. Law enforcement uses the legal system to harass protesters

There are many ways that law enforcement use its powers to stop activists. They excessively investigate, charge and convict activists on trumped-up charges, arrest organizers prior to large protests, and conduct mass arrests of law-abiding citizens during protests. All these strategies were deployed during the G8/G20 protests in Toronto in 2010, for example.

Governments also unfairly apply tax laws to pressure groups to release information, and use grand juries (in the States) to intimidate and silence people and their allies. (Corporations also use civil courts to harass activists, often suing individuals for compensation for lost profits.)

Battling with the courts and spending time in jail is an exceptionally effective way to compound stress and burnout, and redirect a group's efforts to raising legal fees and tackling the legal system. This strategy is commonly used by law enforcement and should be of greatest concern to activist groups.

2. Law enforcement investigates and infiltrates groups

In the pursuit of investigating potential and alleged crimes, police engage in excessive and sometimes illegal physical and electronic surveillance, such as: searching cars and homes, following ("tailing") people, monitoring email and phone communications, and identifying people simply for being activists or attending activist events.

Like The Wire TV series, law enforcement uses informants who are civilians who gather information for the police, usually for money. Anyone can be an informant: your landlord, disgruntled activists, or random students. Police have a tendency to target people with exploitable weaknesses, such as people facing prison time, or suffering

drug/gambling/money problems. It's common for police to offer arrested activists a sweeter plea bargain in return for incriminating information on other activists. Unfortunately, the pursuit of suspected spies can scare off new activists and set off waves of paranoia.

On rarer occasions, law enforcement gathers information through undercover agents who pose as activists. For an extreme example, take police officer, Mark Kennedy, who went deep undercover as a British environmental direct action activist, going to protests around Europe for over seven years.

3. Law enforcement disrupts activities
Infiltrators can disrupt or stymie meetings, and spread malicious gossip and rumors (like accusing others of being undercover agents). This is not law enforcement's primary tactic. These operations are usually organized on a federal level and are longer term. For a recent example, read activist Lisa Fithian's report on the disruptive behavior of a long-time informant named Brandon Darby working on the New Orleans reconstruction effort. (Link: http://theragblog.blogspot.com/2010/03/lisa-fithian-fbi-informant-brandon.html)

Law enforcement also encourages activists to engage in property destruction and violence; these tactics can be used to justify a strong police crackdown and the labeling of activists as "terrorists." Check out this footage (link: http://www.cbc.ca/news/canada/story/2007/08/23/police-montebello.html) of a 2008 protest in Montebello, Quebec, which shows masked-men(one of whom is holding a rock) trying to instigate violence near a police line. After public outcry, the Quebec police admitted the "violent activists" were undercover police. However, this is not the most common strategy for law enforcement to deploy.

4. Opponents and law enforcement engage in targeted excessive force and violence
On occasion, law enforcement harms activists at protests or in jail. In a few cases, law enforcement has also been implicated in assassinations of usually high profile radical activists, such as black civil rights leaders in the 60s and 70s. These strategies are not as common as other law enforcement measures.

HOW DO WE PROTECT OURSELVES?

This guide first outlines some general guidelines, and then offers some specific advice you can take to minimize these threats.

GENERAL GUIDELINES

First, assess your risk

There's no easy answer to the tough question, How security conscious should I be? The consequences of surveillance and harassment have the potential to be severe; however, being overly cautious and constantly preparing for the worst can be debilitating.

Ask yourself, are you at high, low, or medium interest to law enforcement? The table below is a useful guide to help you assess where your group is at.

HIGHER INTEREST FACTORS	LOWER INTEREST FACTORS
Property destruction	Legal protests, eg rallies
Civil disobedience	Research & Lobbying
Poor people	Middle class / Wealthier people
People of color / Marginalized people	White people
Anti-capitalist/revolutionary extremist goals	Moderate, reformist goals
Very politically active	Active on occasion
Minimal public support	Broad public support
Target has huge power, e.g. the military/politicians/police	Target is weaker, with less connections to power-holders, egg. a grocery store

If your group has a combination of higher interest factors then you are more likely to be subject to surveillance and harassment.

If you're not sure you're experiencing surveillance and harassment, and you want an indication of what to expect or prepare for, then look at how law enforcement is dealing with groups similar to yours. (Having said that, past police practice doesn't always predict how police will act in the future.)

It is also useful to gather public information to help you assess how much energy law enforcement could be directing towards your group or issue. Law enforcement often makes public announcements about the size and scope of their security budgets and priorities. In the early 2000s, the FBI was very vocal about its decision to classify extremist animal rights and environmental activists as "terrorists" and quash their activities. Security budgets are usually boosted just prior to high profile national or international meetings, like a G8/G20 Summit or a Republican National Convention, for instance.

Also remember that individuals in your group are subject to different levels of risk. People of color and marginalized people (such as non-citizens) are often of greater interest to law enforcement; some folks are often more vulnerable to the consequences of arrest. (For example, mothers who are arrested and charged with serious crimes are often threatened with losing custody of their children if they don't become informants for the police.)

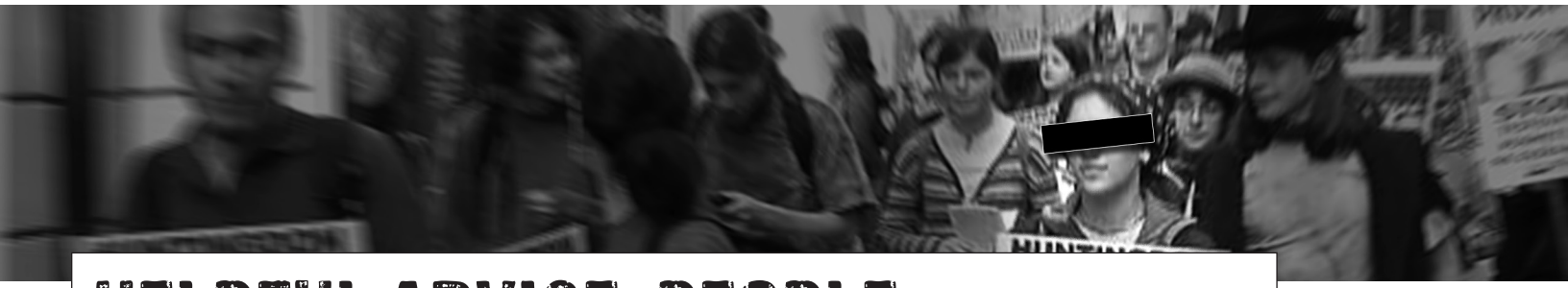
Think through how your group will protect and support your most vulnerable members. For instance, you might choose to avoid putting high-risk people in arrestable positions at protests. Or you might assign more experienced lawyers to represent more vulnerable people in court. There are no one-size-fits all solutions to this dilemma.

Weigh the "pros" and "cons"

Consider whether each security measure is worth implementing, and, if so, make an effort to mitigate the "cons." It is not beneficial to implement security measures to the point where you are spending more energy being "secure" than you are in pursuing your activist goals.

Many security measures are straightforward. It's easy to protect your computer with a complicated passphrase, for instance. Other precautions have negative consequences, taxing a group's time, resources, overall health, and the recruitment of new members.

Some technical fixes (such as encrypting all emails) usually require some expertise in information technology, training and retraining of members, and monitoring, because people forget, get lax, etc. It might be worth adopting these measures if your small group relies heavily on online communication and is conducting a hard-to-execute action that requires surprise (hanging banners off large buildings, for instance). However, some of these solutions don't scale up well. For instance, it is more difficult to implement email encryption if you're working with hundreds of people.



HELPFUL ADVICE: PEOPLE

I think there's an informant in my group. What do I do?

It's a dangerous game to investigate and oust someone as an infiltrator or informant.

First, investigating people is time-consuming.

Second, if you accuse the wrong person, you might lose a valuable activist, and you'll probably ramp up levels of mistrust and paranoia.

Third, it's hard to guess the "undercover." Sure, theories abound…. Your mind might start wondering when you meet people who have access to money, but no obvious employment. Some of us might be curious about people who share no physical evidence (such as parents or high school friends) about life prior to or outside activism.

But these theories are also true for many bona-fide activists. We are not the Mafia. We weren't born into activism, we choose it. Many of us come from elsewhere. Some of us don't talk to our families; some of us have access to money. Law enforcement has proven on many occasions that they can effectively infiltrate our networks and gain our trust with people who both match our theories and disprove them.

Fourth, even if an undercover is ousted, you can never guarantee that you are free from infiltration.

Investigating and outing an undercover agent or an infiltrator might be worth the energy. If you do decide to confront someone you believe to be an undercover, give them a fair chance to defend themselves and provide evidence to the otherwise.

For many high or medium risk groups, it's often best to operate under the assumption that you are under some surveillance.

There are, in fact, many proactive/preventative security measures you can take that can actually improve the effectiveness and well-being of your group, instead of jeopardizing it. We'll turn to them now.

Manage Emotions

Surveillance and harassment generate fear, mistrust, burnout and paranoia. Paranoia is defined as being so suspicious of other people that you are incapable of doing what you need to do. A new member will likely feel unwelcome if they feel they have to prove to everyone's satisfaction that they are not a cop. It is also hard for group members to make sensible decisions if people feel overwhelmed and scared.

Try to keep calm, realistic, and level-headed. There are a lot of resources available on how to stay grounded and calm – from breathing slowly, to taking time to relax and exercise, to just pretending to be calm so your nervousness doesn't spread to others.

If your group is worried about surveillance, embodies many of the factors that make you of interest to law enforcement, or you are actively experiencing repression, talk openly about people's fears and concerns. Talk about realistic and worst-case scenarios. Talking about fears and realizing that other people share your concerns can make these issues less intimidating.

People are often comforted by hearing personal accounts from activists who have experienced and overcome harassment of some kind. Proactively setting up support systems to withstand police interference, such as recruiting lawyers before a mass civil disobedience, can also increase a group's emotional and mental capacity to deal with harassment.

Be nice and supportive

And to continue on this theme of support….

People become informants for many reasons; perhaps they're in a vulnerable position as they are facing prison time, or desperately need money. Common sense tells us that people are less likely to inform on those who treat them with respect, are friends, or strong allies.

Writing letters, organizing fundraisers for legal fees, and visiting activists in jail all help vulnerable people feel appreciated and connected. This makes them less likely to share information about their friends and their movement for a shorter prison sentence. There are many good examples of groups that provide great support for activists experiencing significant threats, such as this one for Briana Waters, who has been battling the legal system for years due to her alleged involvement in environmental activism.

This is stating the obvious (although it isn't always done), but it is also useful to be nice and supportive to people in your group, irrespective of whether they are vulnerable or not. One of the most effective ways to counter surveillance and harassment is to have people remain committed to activism for years (hopefully a lifetime) and to encourage others to do the same. Experience often yields trusting relationships, patience, and perspective. There are many ways to foster commitment, of course, but one useful strategy is to build a group (and activist community) that people enjoy being a part of.

> **REGARDLESS OF WHETHER SOMEONE IS AN INFORMANT OR UNDERCOVER, IF THERE IS A GROUP MEMBER CONTINUOUSLY DISRUPTING YOUR ABILITY TO CAMPAIGN AND FUNCTION IT IS OKAY TO ASK THEM TO STOP, AND, IF THEY DON'T, ASK THEM TO LEAVE.**

Stop bad behavior

Another positive approach to the problem of infiltration is to focus on eliminating bad behavior. Regardless of whether someone is an informant or undercover, if there is a group member continuously disrupting your ability to campaign and function – behaving in a sexist way, lying, constantly gossiping about other group members, failing to do their tasks, and/or rarely following decision-making protocol – it is okay to ask them to stop, and, if they don't, ask them to leave.

This is a great example of a security culture practice that makes you more effective rather than less.

Consider recruitment

Many groups have an open-door policy, where most people can easily join, provided they subscribe to the group's mis-

sion or commit to work. This is great for recruitment and building your group's power. And building your group's power and securing additional support for your issue, is, in the long-term, a very effective way to limit surveillance and harassment.

Other groups set conditions and limitations on who can join. Some people only work with those they have known for many years, others will only work with people who have been vouched-for by a trusted member, or investigated in some way. Other groups will integrate new members in stages. For instance, a direct action activist group in Ontario had a policy of investigating people before inviting them to join their core group. They visited the new activist's house and place of work in order to verify their story, they met the activist's son and girlfriend, and they invited him to participate in public and legal events before allowing him to participate in more controversial actions and civil disobedience.

Strategies such as these generally make it harder for law enforcement to infiltrate. On the flip side, these strategies can make groups exclusionary, can lead to a false sense of security, and often lead to groups recruiting people like them, doesn't lend itself to the goal of building mass public support. If you only need a few people to accomplish your goal then a closed-door policy might be for you, but most groups depend on a constant influx of people and abide by a more open-door policy.

Whatever your policy is, make sure you follow it consistently for everyone who wants to join.

Watch your language

It's best not to say anything you wouldn't want heard used against you in an open court room. That means not talking, bragging, joking or boasting about illegal or sensitive things you (and especially others) have done or might do. Sometimes those statements do end up in court, and the onus will be on you to prove that your comment about hurting cops was just to get a laugh.

Law enforcement has been known to exacerbate divisions between people and groups, by, for instance, spreading unsubstantiated rumors. Don't make their job easier by gossiping or venting. If you have an issue with someone, talk to that person directly. And don't discuss sensitive information, such as the location and time of your civil disobedience, over the phone.

"Need-to-know"

Some groups implement a policy of 'need-to-know', which means people only have access to things they need to do their job. This policy is often employed temporarily, prior to actions that require the element of surprise to be successful, such as a road blockade involving a small number of people. (If you have a lot of people, it's much harder for the police to stop you, even if they do know about the action beforehand.)

Implement this policy in a consistent manner, as resentment tends to build if people see it being applied to some people and not others. That means that even partners and best friends don't get to know the details. Need-to-know also works best when people trust each other and have worked together for long periods.

"Need-to-know" policies can also be applied to the management of data and information. This point is expanded on below.

Consider decision-making and democracy

Repression tends to lead to groups becoming more hierarchical and selective as they want to insulate themselves from disruptive members. Groups might choose to make key decisions in secret with a select few experienced trusted members.

A democratic group with a fair and transparent decision-making process is good for security culture. It is easier to significantly disrupt a group where a few people make decisions (you just have to go for the leader) than it is for a group that shares power and builds leadership.

It is also true that a consensus decision making process can make it easier for one or two dissenting members to hijack the process, by blocking proposals, for instance. This problem can be addressed in ways other than resorting to secrecy or hierarchy. Strong and experienced facilitation can help.

Groups might also choose to transparently modify the decision-making process in some way, perhaps to consensus minus one (which means a proposal is approved even if one person objects) or an 80% voting majority. These measures might be necessary before mass actions where there is a big influx of new people.

HELPFUL ADVICE: DATA

In the course of changing the world, we generate a lot of data. We create everything from handwritten notes on spiral notebooks to digital documents to digital photos to text messages on a daily basis. This data is crucial to our work, but could also be used by our adversaries (law enforcement or private businesses) to sabotage our work, undermine our movement and/or put us in prison.

Everybody knows we need to keep our data secure. Unfortunately, the agreement ends there. Heck, for a lot of us the whole conversation ends there. The practical and legal challenges around data security are so overwhelming that we often don't know where to start, much less where to go.

This section will improve your relationship to data, as an individual and as an organization. You'll not only be safer from the man – you'll also be more in control of the data that increasingly defines how effective we are.

Three principles of data security

Data security – any kind of security – is a rabbit hole you can fall into and never escape from. While some people love to debate the finer points of deadbolts or encryption software, most of us don't have that kind of time. Or paranoia.

There are three complementary ways to think about security. If you keep them in mind you'll always know what direction to go in.

The legal principle: expectation of privacy

Privacy law is one of the most complicated and frequently-changing parts of constitutional law. While lawyers can spend all day debating its finer points, it mostly boils down to your expectation of privacy. The more you can show you reasonably expected privacy, the more likely something of yours the police searched can't be used against you in court later.

In the physical world, if you leave your front door open and let people in and out of your house while you're gone, you're showing a low expectation of privacy. On the other hand, if you keep your backup hard drive in a locked safe in your basement, you're showing a high expectation of privacy. Think about how your actions demonstrate a high expectation of privacy.

One last note: To demonstrate your expectation of privacy, any time law enforcement searches you or your belongings, state clearly and loudly (so witnesses can hear it): "I do not consent to a search." Say this if they're searching you, your car, your house, your tent, your boat or your storage unit. Say it even if you're getting arrested or they have a search warrant. Who knows? Maybe you were just getting detained instead of arrested, or maybe the search warrant had a legal flaw that could only be proven later in court. By saying "I do not consent to a search," you make it clear to the cops and to the courts that you had a high expectation of privacy. Even if the cops still search you, it's less likely they'll be able to use anything they find against you in court later.

The practical principle: Make them work for it

Every security scheme has a weakest link. You might type up your manifestos in a coffee shop where someone could walk in off the street and snatch your laptop. Or you might use the same passphrase for all your email accounts.

The point is not to make it impossible for people to get your data. To do that you'd have to keep everything you know inside your head, never communicate it to anyone else, and then make yourself forget it.

Practical security means that you make the bad guys really work to get your stuff. If they steal your laptop they'll have to get past a wicked passphrase to use it. If they hack your professional email account they won't necessarily have access to your personal account. And that leads us to the next point...

The ethical principle: How will you apologize to your community?

Imagine that you're going to experience a security breach tomorrow. Maybe your house got broken into and the only thing missing is your organization's computer. Or you found out that your email account's been accessed from across the country for the last 2 months. What will you say to all the people you work with and who rely on you?

The underlying principle is being able to honestly say, "We did everything we reasonably could have." You're bound to have data that other people don't want to be made public: Personal text messages, future protest plans, and so on. No one in the modern world expects your data protection to be bulletproof; after all, banks spend millions on security and get hacked all the time.

What people do want is to know that you tried as hard as you could have. If your actions showed an expectation of privacy and that you really made it a challenge for your adversaries to get your stuff, you'll be able to tell your allies that you met that standard. Even if some damage is done in the short term, in the long term you'll all be stronger for it.

Keep them out!

Your first line of defense is perhaps the most important: Keep the bad guys from physically or electronically accessing your stuff.

Physical security

It's easy to overlook the importance of physical security. After all, the internet allows billions of people to have access to our most personal secrets. Having said that, both law enforcement and common thieves have centuries of experience breaking into buildings and taking what they want. (These two parties might seem really different, but if someone breaks into your office and takes your computers, how will you know if it's an act of sabotage or a simple theft?)

At the risk of stating the obvious, you want to make it difficult for people to physically take your stuff. Whether your office is a building downtown or a corner of your bedroom, make sure someone can't just let themselves in. These spaces should be locked securely enough that it would be difficult, noisy and risky to break in – and that, after doing so, there will be evidence people have broken in. (The only thing worse than your adversaries accessing your stuff? When they do so without your knowledge, over and over again.)

Incidentally, good locks and other physical security show an expectation of privacy and make the bad guys have to work to get your stuff.

Portable devices

It's hard to lock down a smart phone. That's almost a shame, because your smart phone is perhaps the single most vulnerable target for law enforcement, private security and criminal hackers alike. The most important thing to do is to have a passphrase or some other way to keep people from just picking up your phone and accessing everything inside. Same goes for laptops. (We'll get to the other important step for portable devices below.) You can also research tools that automatically encrypt your text messages and voice tools. (As of May 2011, TextSecure from Whispered Systems is great for encrpyting text messages; their Redphone app does the same with voice calls.)

But the most important thing is that, if your phone gets lost, stolen, or arrested, the perpetrators won't be able to turn it on and instantly get into your email and bank accounts.

Online services

Speaking of which, the final thing to keep in mind is your online services: Email, eBay, Facebook, Twitter, etc. To make a long story short, have a good, different passphrase for each of these services. - and know that whatever you put online might get surrendered by Gmail or Facebook to authorities without your knowledge. That leads us to the point below...

Managing data

The elephant in the room is your data itself. Here are three simple rules for managing your data.

1. Collect as little data as possible

Don't go around collecting all the information you possibly can. Do you really need a database (or spreadsheet, or Word document) of all of your supporters? Do you need sign-in sheets for every person who's ever come to one of your meetings? If so, that's fine; if not, don't collect it. Minimizing the amount of data you collect isn't just a good habit from a security perspective. It also reduces the amount of time you spend digging through distractions later – junk that can only get in your way and do you and your friends harm.

2. What you keep, keep securely

This is pretty self-explanatory. Make sure your physical data is physically protected and that your online data is protected by good passphrases.

But, this secretly isn't that self-explanatory. Electronic data in particular is slippery. Do the folks in your organization make their own backups of organizational data? If so, do they keep it securely, or are their backups the weakest link? Do they back up to a USB drive? Are sensitive paper documents all kept in a locked cabinet, or are they spread out across the country among members from the last three years? This leads us to our third point below.

3. Destroy your data (securely) as soon as possible

This is the most challenging, but – in the long term – most crucial part of data security. When the authorities want your data, they rarely grab it in a physical search. Instead, they usually send you a subpoena: a court order to turn over what they're requesting.

The first step with a subpoena is to get a lawyer to limit its scope, if not quash it altogether. But eventually you're probably going to have to hand over the relevant documents they request. Most of the time, if you have deleted your information, that's the end of it – even if they could hypothetically take your hard drive to a laboratory and undelete everything.

(People always ask what happens if you don't turn over the documents they ask for. The short answer is that, if you simply refuse on principle, they can put you in jail for a long time, and then possibly turn it into a criminal case. If you destroy the evidence after they ask for it, which is totally illegal, you can go to jail for longer than whatever they initially wanted you for in the first place. As Bill Clinton learned, it's not the crime but the cover-up.)

Speaking of which, your adversaries will sometimes use sophisticated tools to reconstruct data you have attempted to destroy. Whether it's high-powered microscopes that analyze hard drives or computers that digitally stitch together shredded documents, there's a dizzying array of tools at the hands of law enforcement and private corporations.

That's why it's important to securely destroy your data. This isn't hard. For individual files, use a tool that deletes and writes over that part of the hard drive again and again, so those microscopes won't see anything but a bunch of random 1s and 0s. For whole hard drives, take them out of the computer (especially if you're getting rid of the computer), dunk it in water and then smash it with a hammer. (New hard drives are cheap.) For paper documents, shred them in a cross-cut shredder along with a bunch of non-sensitive documents to make the haystack bigger. Or better yet, burn them in a metal garbage can or a fire pit. (See the "How to Destroy Data" section below)

This is a habit your organization and everyone in it has to develop. Delete your old text messages on your phone and old emails that aren't relevant anymore. (Be sure to delete them from your "Sent Messages" folder, too!) (See the"Data Retention" section below)

If you're an official non-profit, keep financial and legal documents for only as long as you are legally obligated to do so. In other words, destroy them as soon as you can. This can be fun! Have an annual purge where you pretend that you're about to get served a subpoena – go through all your documents and destroy the ones you don't need. It can end with a ritual bonfire and hard drive smashing.

Membership

The most challenging part of data security has nothing to do with deadbolts or hard drives. It's membership: who counts as a part of your organization in terms of accessing physical spaces and online accounts. This is a loaded subject because it assumes that people within your group can be a security risk. The unfortunate thing is that that's actually the case. Your members are your most powerful assets, but they – and their bad security habits – can also be your most dangerous adversaries.

Everyone is a security risk

For better or worse, we're all a security risk – not just ex-members or the computer naïve. (Hard core computer geeks often have the worst security habits!) If you keep sensitive emails on your laptop, and then leave your laptop in the back seat of your car where it can get stolen, that's a security risk. If someone is pissed off and leaves the group (or gets kicked out), that's also a security risk. Addressing this question head-on is one of the most effective ways of dealing with this threat without compromising our ability to do work.

"Need to Know" access

The first step is that people should only have access to things they need access to. This may seem obvious, but it's easy to give people access to everything by default – if only to save yourself the grief of meaningfully answering this question.

Your organization needs to take a look at its membership and see who needs access to what resources to do their work. Even your most active members may not need the website passphrase, or the keys to the office.

Be deliberate about entries and exits

Have a consistent process about how people join and leave your group. Literally have a checklist about how people join: Do they immediately get to post to your listserv? Do they get access to your Dropbox account?

More importantly, have a process for how people leave. Have another checklist where, in addition to an exit interview, you ask what organizational documents they still have (and probably get them back), what accounts they had access to and their passphrases (they may have had to create some for the group), collect any keys they have, and so forth.

Then change all the passphrases that person had access to. Do this no matter what the circumstances are. It's tempting to skip this when it's obviously a happy departure. But what about when things are a little unclear? If you send the signal that you only go through this process when you don't trust the person who's leaving, that makes it very difficult to ever use. (See our document "Staff Exit Process")

Act Now!

Don't wait until you're served a subpoena or your office gets broken into. The sooner you take these steps, the quicker you'll meet the principles of legality, practicality and responsibility. Good luck!

Data retention

Your organization probably collects and generates a substantial amount of data, both electronically and on paper.

This includes information about supporters, allies, programs, assets, finances, legal and business relationships, and a wealth of other organizational knowledge. This is the kind of stuff our adversaries in law enforcement and business would love to use against us and our communities.

As an organization, it's your job to responsibly manage and maintain this data.

To meet that responsibility, your organization should have a written agreement on data retention and destruction. This will help ensure that you:

- Keep important documents for as long as you need them
- Get rid of documents you don't need (and could only get you and your friends in trouble)
- Effectively destroy sensitive documents so your adversaries can't recover them
- Have a policy you can point to in court, so the prosecutor can't claim that you selectively destroyed documents because you knew you were breaking the law.

KEEP IMPORTANT DOCUMENTS AS LONG AS NEEDED; GET RID OF DOCUMENTS YOU DON'T NEED; EFFECTIVELY DESTROY SENSITIVE DOCUMENTS; HAVE A POLICY YOU COULD POINT TO IN COURT.

This document is a generic data retention plan. Anything your organization will use has to be customized to meet your needs, agreed upon by everyone who will follow it, and – if you're an official non-profit – run by a lawyer to make sure it's legal. Having said that, this is a good, solid start.

Electronic data

If possible, files should be created and saved to an organizational server, rather than onto individual local computers. Documents and files used in planning events shall be used only during the planning process, and only stored on the server. After the event, all critical information shall be transferred from these documents into the database(s), and then separate documents should be destroyed.

Databases

Contact databases should be used to store all pertinent information on an ongoing basis.

Email

Email should be used for communication, not storage. Avoid emailing documents and sensitive information (including contact information) to other group members. Instead, refer to their location on the server or in the database. Transfer important information from incoming email to the server or appropriate database, and then delete the email immediately.

Instant messaging (IM)

Two specific measures should be taken to maximize the security of instant message (IM) conversations. First, the IM client should be configured to use Off the Record (OTR, http://www.cypherpunks.ca/otr/) in order to encrypt instant message communications. Second, logging of IM conversations should be disabled in the IM application, and remote IM correspondents should be asked to turn off their logging as well.

Physical files

The following physical files should be retained according to legal standards. (Check with a lawyer for state and federal regulations.)

- Fundraising: Major Donors, Foundations, and Events. Event files shall contain attendance lists but no contact information.
- Finances: Accounts Payable and Receivable, Deposit Records, Tax filings, etc.
- Program: Each major event with pertinent planning information and generic budgets; all participant lists shall be removed and destroyed after pertinent information is transferred to database(s).
- Personnel: All employees, contractors, interns, volunteers, employee benefits, etc.
- Administration: Founding documents, insurance, legal filings, services, etc.

Destroying data

By default, all critical information shall be immediately transferred to its appropriate storage site (server, physical file, or database) and then the email or local computer file should be deleted, or paper document shredded, from which the information came. Data will be destroyed on an ongoing, real-time basis.

Removable media

Removable media such as memory sticks, CDs, DVDs, external hard drives, etc. must be maintained securely and regularly to prevent exposure of secure data. Removable

media devices should be treated as the temporary transfer resources they are, rather than as permanent storage devices; therefore, files on rewritable devices should be securely deleted as soon as they are transferred to their approved final storage location, and the devices should be reformatted at least once a month (Windows="format"; Macs="initialize"). Read-only devices (CDs and DVDs) should be saved only as long as needed, and then destroyed (see the "How to Destroy Data" section below).

Other paper

Documents shall be printed only when absolutely necessary and kept only as long as needed. One-sided paper that does NOT contain any travel plans, contact information, critical planning information, financial information, or other sensitive material, shall be re-used for its blank side.

Information on loose paper, message books, notebooks shall be treated as any digital file – important information shall be transferred into a secure storage location, then the original shall be destroyed. (shredded or burned, in this case)

How to destroy data

Effective data security requires thorough destruction of information that is no longer needed. This will show you how to properly destroy different types of data.

Physical data

Once you put paperwork in the trash, it's easy for anyone to grab it. Everything from credit card numbers to strategic plans have been dumpstered by corporate spies or law enforcement. Use the following best practices for destroying physical data:

- Paper files with any sensitive info should be shredded. This makes it harder to decode and shows you have a high expectation of privacy for it.
- Use a cross-cut or diamond-cut, rather than strip-cut, shredder (strips of paper can be easily reassembled).
- Physically mix up the shreds by hand, so the shreds from each page don't get clumped together.
- Using high-tech equipment, even cross-cut shreds can potentially be reassembled. Shred one page of non-sensitive documents for every one page of sensitive documents you shred. This makes your adversaries work twice as hard.
- If you want to be extra careful, you can bleach or burn your shredded paper.

Digital data

When you drag a file to the 'trash' or 'recycle bin' on your computer, it has not actually been deleted. Here's what you need to know to delete fully and with confidence:

- Even when you "empty the trash," your data is not necessarily gone. That part of the disk is simply made available to use for other files. If it does not get reused, the old data is still physically present on the disk and can be retrieved. Even overwriting the data with a new file does not give complete protection.
- When you delete sensitive files, use a program that overwrites the deleted data repeatedly.
- Email gets saved in your inbox (or subfolders). Outgoing mail is often saved locally in a folder automatically by your email program. (Outlook, Thunderbird, etc.) You should check these folders and remove unneeded messages as needed. Better yet, change your settings so they don't get saved by default, or get deleted after two weeks or so.
- Never simply throw out or give away a used hard disk! The best thing to do is to physically remove the hard drive (especially when you're giving away the computer), dunk it in water for awhile, and then smash it with a hammer. For real. (Bonus: this is incredibly satisfying. And they have tiny powerful magnets inside.)
- Data on a CD or DVD should be destroyed by physically destroying the disk. You can use a sander to remove the top layers of the disk; many shredders also accept CD's and DVD's.
- Recent versions of Windows keep checkpoints (copies of the system) at regular intervals that you can restore from. These may contain copies of data you wish removed. Check configuration of these features before editing any sensitive data on these systems.
- When in doubt, don't digitize the data at all!

MEMBERSHIP EXIT PROCESS

Introduction

An organization's membership is its most powerful resource. By the same token, a disgruntled ex-member can be its most dangerous adversary.

Most groups don't have a concrete plan for when someone leaves. Usually the organization doesn't do anything in particular. However, every once in a while someone may leave under questionable circumstances, and the organization will follow some arbitrary steps to try to be more secure.

This is not ideal for a lot of reasons. First, some folks remaining in the organization will feel like that person was being singled out. (Which they were.) Second, the steps you come up with in the moment will never be as well thought out as ones you would come up with beforehand. Finally, just because other folks before left and it seemed okay, they may secretly have been upset.

You should have a process you follow every time someone leaves your staff. This will both keep you as secure as possible and remove the stigma of taking action after only certain individuals leave the organization.

Steps for the member

- Exit interview: Is there anything outstanding we should know about? Do you have any organization-related accounts? – storage/credit/rentals; asset/liability info we should know about that you have and may stop?
- Return organizational stuff from home (physical files, gear, etc.)
- Collect notebooks and physical files
- Gather contact info to give to the organization
- Give new email to forward their old name@organization.org email to
- Schedule going away party

Steps for the group

For computers (If they were using a computer that belonged to the group)

- Transfer organizational data from the person's computer to the organization
- Delete everything from the hard drive (or precise deletion of the person's personal data)
- Re-install the operating system

Passwords/Accounts/etc

- Remove the staff person's name from the website
- Set email autoresponder: "They left, here's their new contact info"
- Shut down their name@organization.org email account after 30 days
- For building security alarms, change alarm system code, if any
- Signatories on financial accounts may need to be changed

RESOURCES

Midnight Special Law Collective provides legal trainings and accessible legal support to activists:
www.midnightspecial.net

The Electronic Frontier Foundation has resources on protecting your online privacy:
www.eff.org

As does **NGOInaBox**:
https://security.ngoinabox.org

and **Access Now**:
https://www.accessnow.org/pages/protecting-your-security-online

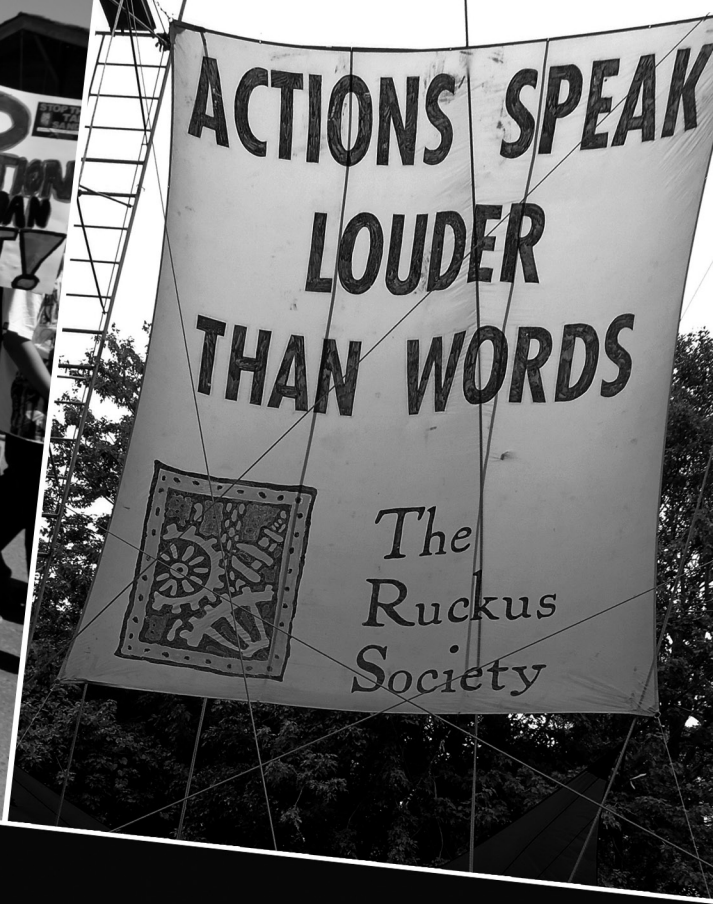
New Tactics in Human Rights lists security measures and links to manuals and downloadable software for data protection:
https://www.newtactics.org/en/blog/new-tactics/staying-safe-security-resources-human-rights-defenders

Resist.ca has a "how to" guide on security culture:
http://security.resist.ca/intro.shtml

Brian Glick authored a useful book called "*War at Home: Covert action against U.S. activists and what we can do about it*".

For current articles on surveillance review reports by **SF Indy Bay**:
http://www.indybay.org/newsitems/2011/06/09/18681443.php

and **Democracy Now**:
http://www.democracynow.org/2011/6/14/fbi_to_expand_domestic_surveillance_powers



THE RUCKUS SOCIETY

Actions Speak Louder Than Words