# Stop Hunting Sheep

## A Guide to Creating Safer Networks

**Stop Hunting Sheep: A Guide to Creating Safer Networks**

**Original text in English**

2011

sproutdistro.com/catalog/zines/security/stop-hunting-sheep

**Layout**

No Trace Project

notrace.how/resources/#stop-hunting

This pamphlet explores the possibilities for countering covert investigative efforts initiated or assisted by police. Sprung from discussions following two police infiltrations into anarchist networks in Southern Ontario[1] in the lead up to the G20 summit in Toronto in 2010, this text offers suggestions on how to start making your networks safer and creating an active security culture within our everyday activities and organizing.

[1] *No Trace Project (N.T.P.) note:* A province of Canada.

# Contents

# Definition of terms

**Informant**: A person recruited by police to provide information.

- Is a member, friend, or associate of the group.
- Is referred to as “Confidential Source” or “Confidential Informant” by police.

**Infiltrator**: A person who infiltrates a group by posing as a genuine member.

- May be military, police, intelligence, corporate, private contractor, “patriot”.
- May be a person facing imprisonment or eviction from the country.

**Snitch**: Someone who gives up incriminating evidence to authorities.

**Snitch Jacket**: Someone who has the reputation for being an informant. It is used both in police jargon and street slang. Jacket comes from the “file jackets” that were used by the police prior to computerization of records. The phrase has part of its origins in the police interrogation tactic of threatening criminals who will not cooperate. Ironically police officers have been known to threaten to publicize or have correctional officers publicize that a perpetrator's “jacket” says they are an informant to get them to inform.

**Network**: A social structure made up of individuals (or organizations) called “nodes”, which are linked (connected) by one or more specific types of interdependency. Radical networks may have complex links based on friendship, sharing living space, common interest, common organizational practice, membership in organizations, shared identity, sexual relationships and connections to a physical space.

**Five basic infiltrator types** :

1. Hang Around: Less active, attends meetings, events, collects documents, observes and listens.
2. Sleeper: Low-key at first, more active later.

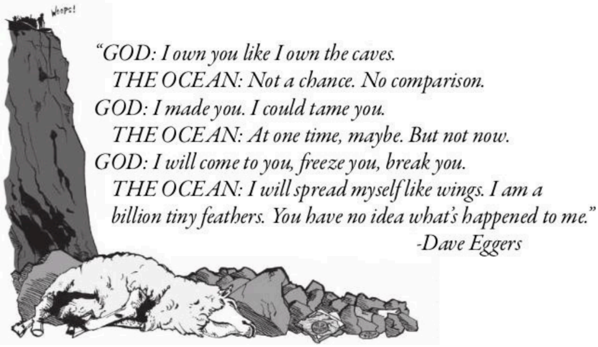
3. Novice: Low political analysis, “helper”, builds trust and credibility over longer term.
4. Super Activist: Out of nowhere, now everywhere. Joins multiple groups or committees. Organizer.
5. Ultra-Militant: Advocates militant actions and conflict. (A variant, the Agent Provocateur: incites illegal acts for arrests or to discredit a group or movement.)

**Light Undercover**: May have fake ID, more likely to return to family life on weekends, etc.

**Deep Undercover**: Has a fake government-issued ID, employment and renting history, etc.

- May have a job, apartment, partner, or even family as part of undercover role.
- Lives role 24-hours day for extended time (with periodic breaks).

# Part 1 : an introduction



*"GOD: I own you like I own the caves.*
*THE OCEAN: Not a chance. No comparison.*
*GOD: I made you. I could tame you.*
*THE OCEAN: At one time, maybe. But not now.*
*GOD: I will come to you, freeze you, break you.*
*THE OCEAN: I will spread myself like wings. I am a billion tiny feathers. You have no idea what's happened to me."*
*-Dave Eggers*

It must be made clear that if there is one thing to take from this pamphlet, there are no fool proof methods for routing out undercover's and informants. This pamphlet is about exploring possibilities for countering covert investigative efforts initiated or assisted by police. The objective of countering all aspects of state-led intelligence gathering is not inherently to reveal undercover activity but to create a safer and less penetrable network to operate out of. Dialogue about this issue need to be addressed with a bit of finesse as there are many dangers, disservices and fruitless avenues people worried about undercover investigative operations can explore. It is clear that our practices in dealing with undercover investigations need invigorated theoretical and practical attention in a manner that we can communicate across our personal networks. In the last several years undercover operatives have been suspected or confirmed in radical networks across the country. In the courtrooms, holding cells and on the gallows, or navigating new worlds free from imposition and misery, we will realize it is only us who can organize our own safety and only our choices that can prepare us for freedom.

There appears to be a rise in known infiltration investigations in North American radical networks, with thorough destabilizing effects on our capacities to struggle, comrades facing heavy repression and of course, the less obvious consequences on our personal mental states. The place that we start is with dialogue. We realize that organizing in radical environments has led many of us to have experiences already with undercover operatives. We have all critically thought about dealing with them, and had personal experience or have heard historical stories of individuals and networks that have dealt with them in the past. We all come from unique organizing environments, and both our networks and police investigative operations are incredibly dynamic. The need for dialogue and personal reflection on methods to provide greater protection for ourselves and the networks we organize out of has become an unavoidable dilemma to confront. Our analysis of the shifting terrain that makes our networks grow and disband, and thorough communication of these understandings to other radical networks are our strongest tools for subverting covert police operations.

A pamphlet that deals with addressing ways to combat undercover investigative work needs to explain the role of an undercover in relation to much broader investigative efforts of police. I.e. undercover's and informants do not exist in vacuums. They are not lone gunmen vigilante types. They are employed in specific investigations to gather information, build cases against people and possibly destabilize the effectiveness of a network. If there is an undercover operative in your network, they are a visible manifestation of a larger investigation which often but not always includes surveillance operations, groomers and handlers[2], and people working on the more technical aspects of information gathering. In the case of a recent undercover police operation, it has been revealed that the undercover was always in very close proximity to two other police officers, while in the presence of people in the radical networks they were embedded in. They also had a handler who they met with morning and night to review notes and make daily objectives, and there were many more police involved in surveillance operations.

There are also various types of covert operatives that have infiltrated and destabilized both radical and criminal organizations. Briefly, there are both shallow and deep undercover's. Informants that range from people imbedded deeply in radical movements that decide to switch sides and build cases as well as former allies that roll under repressive pressure. These

[2] *N.T.P. note:* Handlers are cops in charge of communicating with the undercovers, receiving their reports, etc.

notes only deal with informants and police who are entering networks, not State witnesses and heavily embedded informants who have developed a long history of trust. The question of how to create networks that are uncompromisingly free of snitches, people who cross the line and State witnesses need to be addressed on a more fundamental level in different settings. For various case studies, research Anna Davies, Jacob Ferguson, William O'Neal, Rob Gilchrist, Dave Hall, Jay "Jaybird" Dobyns, Alex Caine, Brendan Darby, Brenda Dougherty, Khalid Mohammad, Andrew Darst.

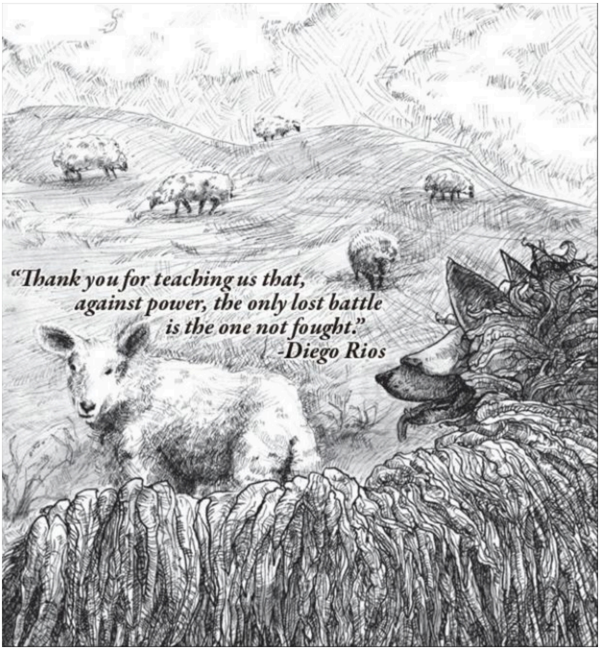
Protecting your safety is protecting everyone's safety. The goal of anarchist agitation is to build a social force that has the potential to destroy hierarchical institutions and paradigms with solidarity. Other goals include: building infrastructure and autonomous space, to intervene in conflict, to push tensions to conflict, and to realize the potentials and interconnectedness of our personal and collective freedom. Anarchists expose that liberal concepts of individual freedom are predicated on dominance and apathy towards others, whereas individual freedom as an anarchist concept cannot be severed from the collective, but can also only be personally defined. An example of this can be seen in offensive struggles and the relevance of solidarity central to the anti-authoritarian spirit. Attacking police for instance in Vancouver, is a direct act of solidarity with people in Guelph or anywhere else who face the same institutions of repression. Through these attacks, the weakening and the example of insolence has implications on the infallibility of police as enforcers of social morality and our collective ability and agency to fight them and win back decentralized control.

On a similar level, our ability to organize ourselves in a manner that is effective in staving off the investigative efforts of the criminal justice system, while maintaining a social presence, is interwoven with our concepts of freedom. I have heard people who have just been dealt the devastating effects of undercover police pillaging their social network say, "the lesson to learn is that I need to distance myself from people I am not confident in and work on projects with people I know well." The issue is that if we see undercover operations as a threat to our personal freedom only, we make half efforts that remove ourselves from danger and leave our networks open to attack. If we individually investigate and critically examine all the links in our networks instead of removing ourselves from parts of them, we provide a greater security to our network and ourselves. We are strengthened by the acts of mutual aid and solidarity, they protect us and at the same time make us more dangerous and uncontrollable.

"Let the pigs join our activist group, they can cook our food and wash our dishes. They aren't going to get shit, because I got nothing to hide." It is still a fairly prevalent idea that covert police investigations don't really harm networks if the more clandestine culture within these networks stays well sealed from the outside. I.e. stick them on the activist groups or if you are concerned about someone, let them stay involved in a peripheral way as long as they don't get close. The concept comes out of the conceited notion that the militant is the center of investigative efforts. This logic does not consider that criminal investigations into anti-authoritarian networks are meant not just to criminalize militant resistance, but destabilize and undermine the networks themselves and create social profiles.

The mentality of the *laissez-faire* anarchist in relation to investigative efforts comes out of laziness, not wanting to upset the herd, not wanting to make yourself look like a person who is concerned about police investigations, not wanting yourself to look like you are snitch jacketing someone, not having the tools to inquire further about someone's background, and feeling helpless or isolated and probably other reasons as well. It is human to have these feelings and rationalities but it is ultimately the most dangerous thing to do. In the absence of being routed out of networks, covert operatives end up building credentials through association, building intensive social profiles on everyone, finding pressure points to cause tension and conflict within networks, entrapping people, and monitoring our daily lives from the comfort of our living rooms.

A final note: There may be people in your network that you are uncomfortable with or find disruptive to organizing efforts. They may not be an undercover operative but still need to be confronted or removed from an organizing capacity to provide safety or a more functional network. Although the goals may not be the same, the destabilizing effects of these relationships on networks have similar effects and should be openly discussed.


"Thank you for teaching us that,
against power, the only lost battle
is the one not fought."
-Diego Rios

# Part 2: the practical side of a safer network

We attend discussions, read information on and do research about the history of repression in radical networks at least partially to learn practical lessons that apply to our life. Below is an attempt to develop an incomplete set of guidelines for discussion which can be adapted and applied to our networks today.

## Building your toolbox

But first, some broad suggestions for tools that may be helpful in aiding personal efforts to strengthen one's safety:

- Understand and research the different types of risks that are posed from undercover's, informants and State witnesses.
- Research the historical case studies and impacts of undercover's, informants and snitches on social movements and underworld tendencies.
- Review relevant police literature on investigative techniques, to gain insight into ways undercover police operations may function and to develop investigative techniques to use in combative ways and gain security.
- Review literature and ongoing discussions related to security culture[3].
- Examine the history of organizing methods used in radical networks, revolutionary organizations in different eras and places and compare them to modern affinity-based organizational models of today's anarchist networks.
- For historical examples research: OCAP[4], Os Cangaceiros[5], Rote Zora[6], the A.L.F[7]/E.L.F[8], the Red Army Faction[9], The I.R.A.[10], the Black Panther Party[11], Insurrectionary Anarchism, Autonomist movements and Anti-fascist resistance in occupied Europe during

WWII. Or read books such as We Are An Image Of The Future[12], The Subversion Of Politics[13], Agents of Repression: The FBI's Secret War Against the Black Panther Party and the American Indian Movement[14], Black Mask & Up Against The Wall Motherfucker[15], Argentina's Anarchist Past: Paradoxes of Utopia[16], Confronting fascism: Notes On a Militant Movement Direct Action[17], etc.

## Guidelines

"It is easy to hit a bird flying in a straight line."

— *B. Gracian*

[3] *N.T.P. note:* For a list of publications related to security culture, see the corresponding topic[18] on our website.

[18] https://notrace.how/resources/#topic=security-culture

[4] *N.T.P. note:* Ontario Coalition Against Poverty, an anti-poverty group in Ontario.

[5] *N.T.P. note:* A group active in France in the 80s and 90s.

[6] *N.T.P. note:* Feminist armed organization active in West Germany from 1974 to 1995.

[7] *N.T.P. note:* Animal Liberation Front, term used internationally to claim actions related to animal liberation.

[8] *N.T.P. note:* Earth Liberation Front, term used internationally to claim actions against the exploitation and destruction of the environment.

[9] *N.T.P. note:* Far-left armed organization active from 1968 to 1998 in West Germany.

[10] *N.T.P. note:* Irish Republican Army, named used, since the beginning of the 20th century, by various armed organizations struggling against British imperialism in Ireland.

[11] *N.T.P. note:* Revolutionary *black power* movement active in the United States in the 60s, 70s and 80s.

[12] *N.T.P. note:* About the 2008 uprising in Greece. Published in 2008.

[13] *N.T.P. note:* About various European autonomous movements starting from the 70s. Published in 2006.

[14] *N.T.P. note:* Published in 1988.

[15] *N.T.P. note:* About two groups, "Black Mask" and "Up Against The Wall Motherfucker", active in New York, United States, in the 60s. Published in 1993 with a new edition in 2011.

[16] *N.T.P. note:* About the anarchist movement in Buenos Aires, Argentina, between 1890 and 1910. Published in 2001, English translation published in 2011.

[17] *N.T.P. note:* About fascism and anti-fascism. Published in 2002.

These are six guidelines for developing safer networks. There will never be single solutions. This model may provide suggestions that guide a more secure practice. Ultimately, these structured ways of creating more secure networks must be very dynamic to stay relevant. As investigative efforts adapt, so do our practices to stay ahead.

1. Creating a "base of safety" list
2. Creating a network map
3. Tactics for further inquiry
4. Communicating with your base
5. Communicating with a potential police informant
6. Concluding action if undercover informants are discovered

## Creating a "base of safety" list

Create a list of people that are involved in your networks. Ask yourself a series of structured questions which reveal your level of safety with each individual in the network.

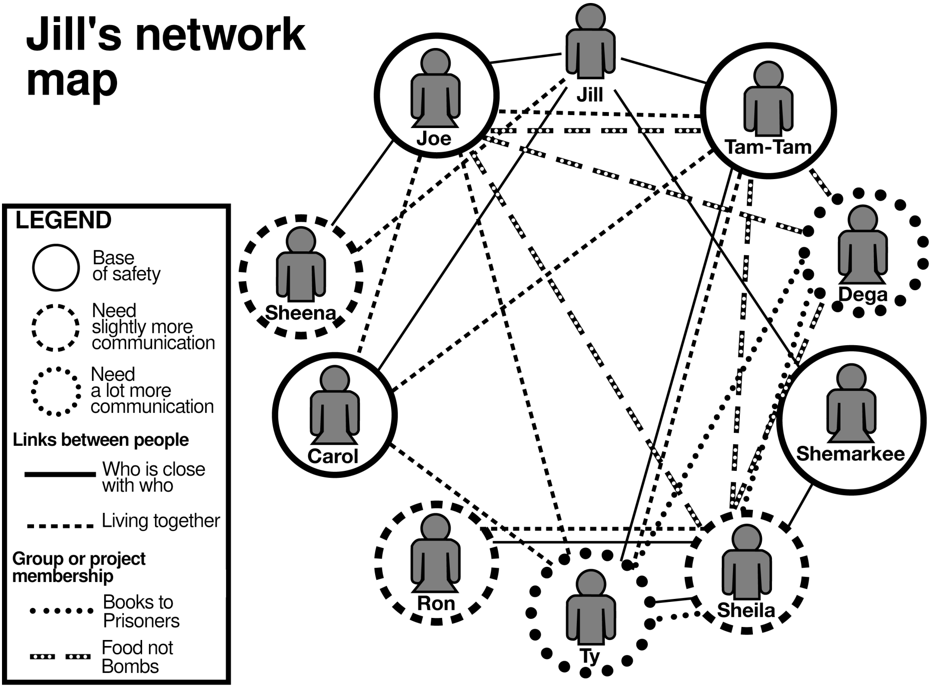
- Who are the people close to you?
- How do you know them?
- Who are your comrades (people you work on projects with)?
- Who are the people you likely enter confrontation with?
- What is their historical connection to you?
- How did you meet, where did you meet?
- Through which people were you introduced?
- Have you met their other friends from different social networks?
- Have you met their families?
- Can people you trust verify their history?
- Are there aspects of their life you have a hard time communicating about or verifying (work, home, vehicle, aspects of their past)?
- Have you clearly talked about and are satisfied with the intentions of the people you organize with on the projects you mutually work on?

- Do you like how they communicate to others about similar experiences you have had with them?
- Do you have a strong sense of trust? Why?

You will now have divided lists of people. Some of which you were at ease answering the above questions for and feel very secure and trusting with: this is your “base of safety”. Other people on the list you may know varying degrees of information about but have revealed that aspects of their life or the way you relate to them may be aloof to you. You want to communicate more with them before adding them to your “base of safety”. You will realize that a hierarchy of knowledge and safety will probably develop, where some people may just need small conversations to feel more secure with, and other people may need a lot of effort to reveal safety. On a personal level investigative lists like these are formal extensions of our choices in association we make mentally on a daily basis. This exercise is to sharpen our ability to make informed and critical choices about the people we associate with. The goals in these assessment questions are to critically understand the social relations that make up day-to-day interactions with the broader network you commonly relate to. Analyzing relationships in this manner may be effective in both mapping and realizing a network of relative safety, while exposing aspects of people you want to learn more about in the hopes of them becoming safer links in your network. The use of exercises like this affirms a base of safety and allows for pro-active individual research, preferably in periods of relative calm. Taking the time and energy to do this work are steps towards critical and empowering choices related to our safety that steal agency from the grips of paranoid haplessness and fear.

## Creating a network map

# Jill's network map



Place the list of people in your network on to a network map. Use 3 different color pens or markers to write people names on the map, depending on whether they are on your "base of safety", or someone you would like to know more about before adding them to your list.

- Color 1: "Base of safety"
- Color 2: People that need slightly more communication.
- Color 3: People that require a lot of communication.

Now create links using more colors to reveal the perceived connections of people within the network.

- Color 4: Who lives together
- Color 5: Who are people closest to you in the network.
- Color 6–?: Use markers to define project membership to the best of your ability. I.e. a marker will be used to connect the members of your local Food Not Bombs group[19], while another marker will be used to define the Books to Prisoners group[20].

Note: It would be foolish to include clandestine organizational efforts in this list[21].

Your completed map will now reveal several details:

- The level at which people are embedded in your networks by the amount and types of links they have.
- The types of social connections that people have to each other in a network.

It could reveal…

- That someone you are interested in more communication with is also close to people that are on your "base of safety".
- There are people you or other people in your base of safety organize with that have tenuous social connections.
- That you need help from people in your "base of safety" to assist in the inquiry?

## Tactics for further inquiry

It is imperative to see the people you want to know more about as people with the potential to be in your safety network. If you believe that there is no way you will ever feel safe with that person in your network, there are probably more issues than just untrustworthy behavior. Consider talking with very close friends from your "base of safety" about options, such as, removing that person from your network, or having a discussion with the person around why you do not want to organize with them.

[19] *N.T.P. note:* Network of collectives that cook and/or share free food.

[20] *N.T.P. note:* Term used by groups who sent books to people in prison for free.

[21] *N.T.P. note:* We do not necessarily agree with this claim. Including a clandestine effort in the network map can be useful, for example if it reveals that links between certain members of the group aren't as strong as you thought. Such information would of course be valuable for the police, but such is the case of any network map. Our main advice would thus be to remember to destroy the map immediatly after finishing the exercise, for example by burning it.

## *Soft questions*

Soft questions are meant to be asked in subtle and undetected ways and are aimed at revealing information in a way that masks intention of the questioner.

Think about the environment and atmosphere and attempt to control the environmental variables for the questions. A relaxed and comfortable person is more likely going to have their guard down. They are more likely going to indulge you to keep up the pleasantries of conversation. It is also impossible to detect shifts in body language and facial expression when people are stressed out. Subtle and benign questions focused around the direction of aspects of their life that you would like to know more about may help. If you want to understand their past better, for example, during a friendly conversation you could steer the direction of conversation to your family history, and maybe ask questions like: What is your mom's name? Did she keep her maiden name or is that your dad's last name too?

## *Hard questions*

Hard questions are meant to be interrogative. They are meant to put the person you are communicating with on edge, to let them know that you are serious about retaining information[22].

These types of questions are aimed at revealing information through implied coercion. They work with questions that you can verify in the moment. Where were you born? Where did you go to primary school? What is your birthday? What is your middle name? What job do you have? Give me your parents phone number and wait here with me while I verify the information…

[22] *N.T.P. note:* Another zine, "Confidence. Courage. Connection. Trust. A proposal for security culture[23]", details a different approach that consists in using explicit questions to check someone's identity—that is to establish that a person is who they claim to be—as part of a mutual process between people who trust each other. We find the mutual approach sometimes more relevant than the "coercitive" approach described here.

[23] https://notrace.how/resources/#confidence-courage-connection-trust

### *Physical surveillance*

It is also possible to put in place physical surveillance of a person to learn to know them. To do so, the following information can be useful:

- License plates and VIN numbers.
- Addresses (to visit them or check their garbage).

## Communicating with your "base of safety"

> "I think she's a cop."
>
> "Why?"
>
> "Did you see the clothes she was wearing, and she asked me what I thought about how the demo went."
>
> "Dre you wasted!"

Contrary to the very common, very uninformed snitch-jacketing that goes on in anti-authoritarian networks, we need to develop a security model that limits paranoia through gathering intelligence and communicating in ways that refrain from alarm and sensationalism.

All communication approaches are contextual, these suggestions are based on personal experience and reflection and may not apply.

The importance and delicacy of communication with your network can not be understated. Security issues have a way of bringing out irrational, frustrated and upsetting tendencies within most people. It is hard to broach a conversation that focuses on the idea that a person you know could potentially be manipulating and deceiving you for malicious purposes; it can in many ways can cause strong tension and divisions amongst the network.

In my experience with conversations related to dealing with potential undercover's, there was always a strong sense of division and frustration amongst close friends on how to approach the person, if at all. With this knowledge, think about ways to disarm and de-escalate potentially divisive conversations with people before you have them. The place to start communication is on the ground floor of general inquiry with explanations that build cases for more research on an individual or add people to a position on your “base of safety”.

Think hard about how you want to reveal information you have to your very closest comrades, to people who are closest with people you are inquiring about, and of course to the individual you are interested in with the goal being a zero tolerance for gossip and hurtful rumors. The objective of good communication as is the objective of countering all aspects of State-led intelligence gathering is not inherently to reveal undercover activity but to create a safer and less penetrable network. This desire for personal and collective safety can be helpful in communication with hostile people in the network over the desire to find a rat that may not exist.

## Communicating with potential undercover operatives

- Know that if they are in your presence and they are working, they very well may not be alone, in terms of recording devices or unseen law enforcement.
- Wait for confirmation before allegations.
- Watch the ways you threaten people and make choices based on well thought out plans. Intimidating a peace/police officer is becoming a more widely used charge.
- Not revealing intentions and a friendly attitude can be more appropriate for gleaning information than interrogative communication.

## Concluding action if undercover informants are discovered

## Case studies

On the U.S. East Coast a FOIA[24] request led to the deduction of an operational informant, and through investigative efforts they narrowed their search and surveilled a potential informant until confirmation.

In Pittsburgh during the lead up to the G20[25] a pop questionnaire was put on everybody that attended a meeting. When one person could not answer the questions adequately, they were asked to leave the meeting and disappeared from the network.

When traveling to some networks in Europe it is common for people to ask you for background checks involving phone numbers of people close to you and other verifying information before you enter the network.

[24] *N.T.P. note:* Freedom of Information Act, U.S. law that forces federal agencies to transmit their documents to anyone on demande, under certain limits.

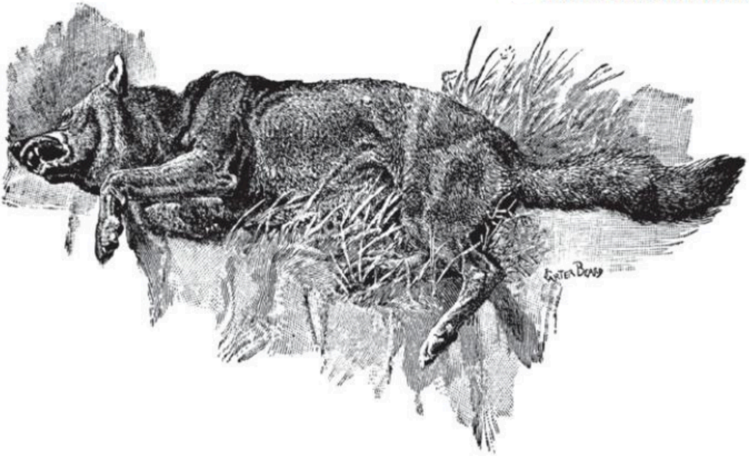
[25] *N.T.P. note:* The city of Pittsburgh, in the U.S., hosted the G20 summit in 2009.

A license plate check through the Ministry of Transportation in Ontario may reveal who the owner of a car is, and whether the car is a fleet vehicle or belongs to a company that deals with law enforcement.

Research in Guelph (in Ontario, Canada) related to verification of Brenda Dougherty as a student at the local university, could have outed her as an undercover as early as September 2009.

*"Let us speak, though we show all our faults and weaknesses, - for it is a sign of strength to be weak, to know it, and out with it - not in a set way and ostentatiously, though, but incidentally and without premeditation."*

***Herman Melville***



This zine is about exploring possibilities for countering covert investigative efforts initiated or assisted by police. The objective of countering all aspects of state led intelligence gathering is not inherently to reveal under-cover activity but to create a safer and less penetrable network to operate out of. This zine offers suggestions on how to start making your networks safer and creating an active security culture within our everyday activities and organizing.

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

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