Security for Climate Campaigners

Disclaimer: everything in this document is for information purposes only. Please do not use it to do anything illegal, but protect your right to protest and change the world for a better place. We cannot take responsibility for your actions, though we say that you should be as active as possible.

WHY SECURITY?

Security is important as we live in a world where upsetting the status quo to change the world for the better is generally met by a backlash. Governments, law enforcement agencies and corporations all have vested interests in criminalizing, disrupting and suppressing activist groups of all persuasions. Security is needed to ensure our continued success, and it is our basic human right to protect ourselves from unwarranted intrusion.

For those who say that we shouldn't have anything to hide or should make a principled stand on it, well we live in a world where democracy is subverted daily and the people doing it the most are those in power. As long as governments and their supporting apparatus permit corruption through their closed and secretive natures then we need to respond in kind for our own protection.

Threats do not just come from the state. There are situations where media organisations with their own agenda will attempt to target campaign groups. Private investigators also need to be factored in as threats. Both have distinct issues which also need to be dealt with to ensure your message successfully gets to the public without being intercepted or disrupted.

Security is a *process* that protects you in some fashion, whether in the run up to, during or after the event(s) you are involved in. This means that security is there to *facilitate* the smooth operation of your action, campaign, etc. and help keep everyone safe. Decisions about security touch on many areas. Security is itself a complex political and ideological area and it is important for individual activists to take on board the issues raised and consider them in an informed way before making personal choices about their own views, and to be aware about how this position will affect others they are working with.

A common mistake is equating paranoia with security. Paranoia is often used as an excuse not to take action through fear of what can go wrong – normally by over-stating the omnipotence of opponents. In our experience paranoid people have little to fear as they are too nervous to do anything that would actually put them at risk. Indeed, few even have security measures put in place. This sort of fear means you effectively defeat yourself.

There is no such thing as a 100% fail-safe system, and not doing actions because you cannot reach that level of security is not an excuse for copping out. There is always some risk; and security processes help reduce that risk to an acceptable level. It is up to you to define what the acceptable level of risk is and how best you can deal with it. Sometimes you just have to take a chance.

Security is not a single thing; it is a *process* and a *state of mind.* The secure activist will be more effective in the long term. The level of security you are working towards obviously depends on the types of action you are taking, and it is often a contentious issue. For example, through the climate

camp, we aim to inspire individuals and promote direct action. Therefore, it's important to be inclusive. But it's also important to be realistic about threats we face. To protect ourselves for the future, and to be effective, it is important to think carefully about the repercussions of what we do.

Thinking about security should in no way stop you from doing an action, and it is really important to consider the level of security required for your action. For example, if you are planning a demo, you do not need to necessarily use clean action phones for all communication, or only discuss details face to face (although you may wish to). If too much time is spent thinking about security then this is a major victory for the state, or whoever is tying to obtain information on you and your activities. Therefore, it is vital in all the work that you do to consider a level of security that will protect you if necessary, but will not inhibit your activities, or be too complex as to divert you from the task in hand.

The ideas presented here are merely suggestions, and may seem over the top to certain individuals. But unfortunately, as recent actions have shown, we live in a time where police are increasingly interested in our actions, and are extremely effective at gathering data. There is nothing worse than spending time, money and energy planning an action only to find the police know all about it. In order to build a successful movement, it is important to build a secure culture for our long term effectiveness.

Below is a simple set of guidelines to make our campaigning more successful and secure. For more information check out the resources at the end of this document, and especially http://www.activistsecurity.org

1. A good tip is for each group to consider any risks they may face and what are the best ways for that group to deal with as a whole – also take into account your interactions with other groups.

2. If you know anything sensitive about your campaign or planned action keep it to yourselves. If you hear anyone else passing on sensitive information ask them to stop.

3. Only give out information that has been publicly disclosed, regardless who it is to. Don't make unilateral decisions about disclosure, but discuss within your group what information is public and what is to remain private.

4. Don't give out other people's names without their permission.

5. If your group has a dedicated mobile phone/email address use it as much as possible. Why not use an alias?

6. Delete unnecessary emails as soon as possible.

7. Don't say anything over the phone or email you would have difficulty justifying in court or would land others in trouble.

8. If using email consider using PGP encryption or dead-mail drops were you leave messages for each other in drafts folders.

9. Don't hand out other people's details without their express permission. If people don't need to

know, then don't tell them personal information.

10. Mobile phones are bugging and tracking devices – leave them behind if you don't want to be tracked.

11. Burn sensitive information.

12. Make sure that you tidy up after yourself following meetings – for example, do not leave invoices / lists of email addresses, etc lying around.

13. If you are planning an action, then you need a different level of security altogether. If you are in doubt, get advice. Check out http://www.activistsecurity.org

Security is about taking precautions in order that you remain effective – what it is not is paranoia. Security will also take a bit of time and effort. There is no way around that and there are no short cuts, but if it is built in from the beginning and everyone agrees to it then it becomes second nature.

Resources for Security

www.activistsecurity.org - security for activist's site –
Still being built, but contains a comprehensive briefing on security issues. Edited handbook coming soon!
www.mcspotlight.org/case/trial/story.html
- Story of the McLibel case, including information about infiltration.
www.freebeagles.org/articles/mobile_phones.html
- Playing safe with mobile phones. Not that unto date but useful background information.
www.angelfire.com/pe2/peaceproject/activ.html
- An article about covert activities against activist groups - including lots of useful web links to other good articles.
www.theregister.co.uk/2001/09/06/eu_releases_echelon_spying_report/
- Article on EU report on Echelon (plus link to EU report).
www.no2id.net/
-Campaign against Identity Cards in the UK.
http://indymedia.org.uk/en/2004/10/300000.html
- Account of how police intercepted a covert GM action.
www.eco-action.org/rr/ch13.html
- Road Raging section on Campaign Security. Old, but still relevant!
www.evel.nl/spinwatch/TRFrontpage.htm
- Eye opening account of big business infiltrating and incapacitating protest groups

Computer Stuff

www.pgpi.org/
- Get PGP for Windows (for Linux, use GPG and look in your

distribution disks!)
www.shac.net/pgp
- How to use PGP for Windows.
http://anon.inf.tu-dresden.de/
- Free Anonymous Proxy (anonymous web browsing).
http://www.theregister.co.uk/security/security_report_windows_vs_linux/
- Report comparing security of Windows and Linux.

Recommended Reading
http://news.com.com/2100-1029-6140191.html - full story on bugging switched off phones

http://www.ft.com/cms/s/4239e29e-02f2-11da-84e5-00000e2511c8,dwp_uuid=4e612cca-6707-11da-a650-0000779e2340,print=yes.html
FT article from 2005

http://yro.slashdot.org/article.pl?sid=06/12/02/0415209
FBI Taps Cell Phone Microphones in Mafia Case
On December 2nd, 2006 with 274 comments includes links to the judge's findings

http://yro.slashdot.org/article.pl?sid=06/12/04/0456220
How To Tell If Your Cell Phone Is Bugged

http://news.com.com/2100-1029-6140191.html Full story on bugging switched off phones.

Battling Big Business - Countering greenwash, infiltration and other forms of corporate bullying, edited by Eveline Lubbers, Green Books, 2002, ISBN 190399814X

Data gathering:
http://www.netcu.org.uk/default.jsp NETCU
http://en.wikipedia.org/wiki/Forward_Intelligence_Team FIT