The Anti-Frackers Guide to resisting police surveillance

NET POL

netpol.org

2015

Contents

Organising Online

Organising Public Events

Organising Online

- Think about how you communicate online and who within your group takes on this role
- Understand the different privacy settings for Facebook and consider other, more secure options for online organising.
- If you are using tools like Twitter, YouTube or Instagram, make sure you are not posting updates, photos or videos that allow the tracking of your location or that incriminates others.
- Remember that if you are arrested, the police can obtain large amounts of personal data about you from your smartphone.

Online police intelligence gathering

Since the riots of 2011 and boosted by Home Office funding before the London 2012 Olympics, most police forces have purchased software and employed staff to gather 'open source' intelligence from social media such as Twitter, Facebook and YouTube. This even has an Orwellian-sounding name: SOCMINT (Social Media Intelligence).

Gathering large amounts of data and then subjecting it to extensive analysis enables the police to build profiles of campaigning groups and the relationships between groups; to predict the size of protests and who is likely to attend them; and to measure early signs of community anger or mobilisation about a particular subject or issue. Using geo-location data it is also possible for intelligence-gatherers to map out, for example, tweets or uploaded videos in real time.

For individual activists, 'open source' intelligence can also help with the creation by police of a 'subject profile', which can include details of family and relationships; lifestyle and habits; employment details; and personal finances.

The problem for activists is that sharing information on social media has become an essential part of modern campaigning: online debates are where large numbers of people now regularly talk to each other.

It is true that police can and do direct online intelligence gathering at individuals and you can find more information to guard against this at the Activist Security Handbook website at **www.activistsecurity.org**. However, much of the data collected by the police does not require 'covert' measures – we hand over information about ourselves online all the time.

There are therefore some simple steps to consider when using social media:

Think about how your group communicates

Encourage your campaign group to decide early on what information is intended for public access or internal use and allocate the role of external communication (including social media) to a member (or a team) within your group, preferably people who are also proficient in dealing with the media.

It is always more likely that your 'overt' data security is compromised by inexperience and lack of preparation.

Think about how your campaign uses Facebook

Most activists who use their Facebook accounts do so for both personal reasons and for campaigning. You may wish to consider how best to separate the two – and how you use Facebook for promoting a campaign and alternatively for the practicalities of organising it.

Facebook is a useful platform for publicising your campaigning activities but you should consider whether it is also the best space for organising. You may want to think about using alternatives such as Crabgrass, Basecamp, Pidder or other closed, more secure sites.

Crabgrass on RiseUp: https://we.riseup.net/
Basecamp: https://basecamp.com/
Pidder: https://www.pidder.de/en/index.html
Trello: https://trello.com/

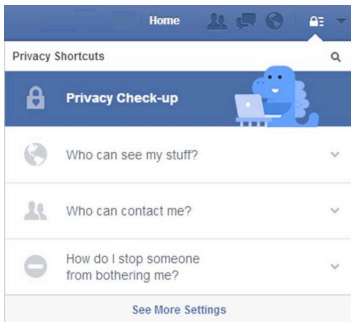
If your group is using Facebook for anything other than a 'Page' to promote public activities, such as a Group, look carefully at its privacy and consider whether the membership of a group that, for example, focuses on practicalities like lift-sharing (and therefore reveals individual activists' travel plans) is better 'secret' or 'closed'.

A summary of the difference between group privacy options is available at **http://tinyurl.com/netpol-facebook**

If you create a Facebook Event, consider hiding the guest list.

Using Facebook as an individual activist

Click on Privacy Check-up (in the top right of Facebook) and edit who can see your future posts and who can look you up. You can restrict others from posting tagged pictures of you without your permission.



You can find more about individual privacy options at **https://www.facebook.com/about/basics/**

Consider setting up a list of trusted Facebook friends for certain updates relating to anti-fracking campaign activities.

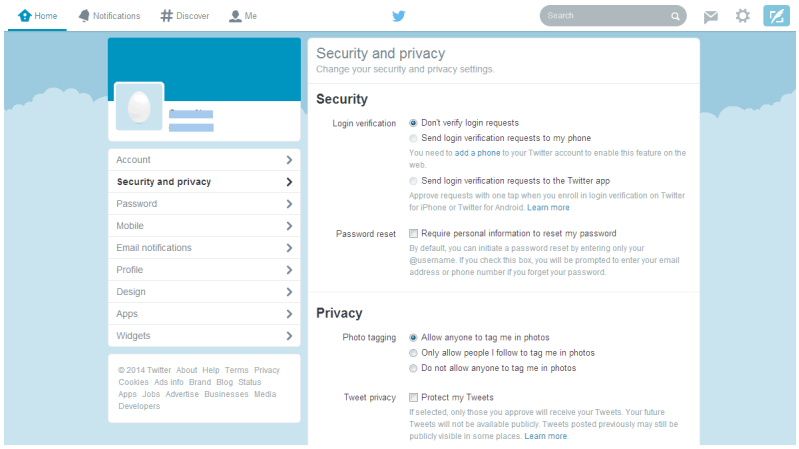
Avoid using location tags in your status updates and prevent others from doing so without your permission by enabling 'Timeline Review'. If you are using Facebook on your phone, turn off GPS location settings

Make sure that you are individually aware that posts you make in debates on public Facebook Groups or Pages you join or 'Like' are viewable by anyone.

Sharing on Twitter, YouTube and Instagram

Twitter is an effective communication tool for activists but unless your account is locked (making it inaccessible to many of those you most want to communicate with), it is also a very public source of information for the police about whom you are talking to.

To begin with, update your privacy settings. Go to your account and select 'Security and Privacy' and select 'Do not allow anyone to tag me in photos', as well as deselecting 'Add a location to my Tweets' and the 'Discoverability' options. You may want to choose to delete all location information from previous tweets too.



Whether you are using a personal or campaign Twitter account, think carefully about the way you use it and the information you include in tweets:

- Is it a good idea to mention publicly, for example, where you plan to meet other activists before or after attending a demonstration?

- 'Live-tweeting' a protest may help to raise its profile but is it also giving a blow-by-blow account of real-time events that helps place you at a particular location and the police to make arrests and contain or stifle the protest itself?

- Would it be better to ask another user to communicate via a Direct Message or to suggest discussing an issue further by email, rather than replying to a tweet publicly?

- Remember that mentioning other users in tweets helps to establish a link between you and them. If they are less careful about revealing their location or, for example, discussions at a meeting, this can inadvertently help to

reveal information about you that is beyond your control. If in doubt, avoid tweets along the lines of "Great to meet up with @policemonitor today" unless you know the user is as concerned about online privacy and security as you are.

- Remember too that the use of a Twitter hashtag (for example, #COP21) can locate you at an event or protest even if GPS location information is turned off on your phone.

  You can check the level of risk that geo-tagging is identifying your movements at **http://geosocialfootprint.com/**

Think carefully about photos or videos you share on public online spaces like Instagram, Flickr, YouTube and Twitter. As well as inadvertently sharing potentially incriminating evidence (see below) that could lead to someone's arrest, data protection subject access requests have revealed that photos from social media have been used to help police Forward Intelligence Teams to identify individual activists. If you post a photo or video, ask yourself: is it necessary to name the people in it?

Log out of apps – or leave you smartphone at home

If you are taking part in a protest and you have a smartphone with you, log out of apps such as Uber or Google Maps that you have given GPS location permissions to. For an extra level of security, delete the apps you never use and avoid adding free apps that include ads: they tend to track your location for targeted advertising purposes.

Signing out will (usually) stop the delivery of your location data to that app's server, so that if the police then obtain a warrant forcing the app service to hand over your data from their server, they will have nothing to give them.

If you are taking part in protests that have a greater likelihood of arrests, the best option is to avoid taking a smartphone completely. If you are arrested, the police can download all information from smartphones and have access to emails, phone logs, contacts, text messages and photos, as well as full access to your Facebook account.

Police enforcement of online material

Police can use information gathered from social media as both evidence in an investigation of an alleged public order related offence and to bring charges arising specifically from material posted online.

Providing the police with incriminating evidence

As well as helping the police with 'open source' intelligence, there is a risk that sharing photos or video online can provide evidence for prosecutions of individual activists. Video taken with a smartphone is the greatest risk: whilst it can help to highlight oppressive policing and police violence, it is difficult to control what you film and the police can seize footage if they think it contains evidence.

Think carefully before posting video or photos online and consider whether a photo or video clearly identifies other activists, particularly in the prelude or aftermath of a direct action or during an arrest.

The general advice is: if you are not sure, don't take the risk and don't post it online.

Prosecutions for material posted online

In 2013, the Crown Prosecution Service issued guidelines on prosecutions relating to communications via social media, which can include

- Credible threats of violence to the person or damage to property
- Specifically targeting of an individual or individuals that may constitute harassment or stalking under the Protection from Harassment Act 1997
- Breach of a court order
- Communications may be considered "grossly offensive, indecent, obscene or false".

Section 1 of the Malicious Communications Act 1988 prohibits the sending of an electronic communication that conveys a threat and section 127 of the Communications Act 2003 prohibits the sending of messages of a "menacing

character" by means of a public telecommunications network. The courts have established, however, the alleged threat that is not ‘credible’ or lacks menace should fall outside the limits of this legislation.

The CPS insists there is a high ‘evidential threshold’ for bringing a prosecution in order to protect freedom of expression, but in a heated local campaign over a fracking site, there is a risk of the police pursuing investigations for alleged online intimidation or harassment of fracking company staff workers or local residents (unsubstantiated allegations of this kind were levelled at Barton Moss protesters). The police may also decide an inadvisable announcement on Twitter of an intention to destroy drilling equipment at a site (or inciting others to do) is a credible threat to damage property.

In all of these instances, encouraging activists to avoid unnecessarily incriminating themselves because of the possible consequences is a useful part of your campaign’s approach to communication and your activist training.

Organising Public Events

- You can ask uniformed police officers to leave a public meeting if there is no likelihood of a breach of the peace.
- If the police are filming or photographing people arriving or leaving a meeting or event, remember you can lawfully cover your face.
- If the police use stop and search powers to gather intelligence, you are not required to give your name and address (unless you are the driver of a vehicle).
- If officers visit you at home, you do not have to talk to them or let them in – but you can quite lawfully film them.
- If your campaign would benefit from 'Know Your Rights' training, contact Netpol.

Organising a gathering, meeting or conference

Finding a venue

Finding an appropriate and affordable venue is often the most difficult part of organising any public event and unfortunately, this can be even harder if the meeting or conference is related to protest or activism. Venue managers may become nervous of their venue becoming the focus on an anti-fracking group, or that they may attract the attention of the police.

Booking without complete openness about the purpose of your event is a legitimate reason for the venue to cancel if leaned on by the police. It may therefore help to provide reassurance by explaining exactly what the event you

are holding is about, the numbers of people who will be attending and what steps you plan to take to ensure any conditions are met. This could include arranging your own security or an offer to pay a deposit.

Police 'disruption' of meetings

There have been a number of occasions when police have approached the venues hosting political or protest planning meetings, to express concerns or to ask for information – such as the name of the person booking the rooms. In some cases, this sudden interest by the police has resulted in venue managers pulling out of bookings, sometimes at the last minute.

For example, a 'mini-peace festival' planned in 2014 for Bridgend in South Wales was abandoned when the pub hosting the event withdrew support, after police expressed unspecified 'concerns' that were never made public.

It is also not uncommon for police to approach landowners who have agreed to allow environmental camps or gatherings on their land, sometimes resulting in the rescinding of permission.

It is difficult to avoid this sort of eventuality – but providing reassurance and establishing good communication with venue managers and landowners is always helpful.

Police attendance at meetings

It is difficult to control attendance at public meetings, but you can ask uniformed officers to leave if there is no obvious reason for them to be there. The law says police must have a genuine belief that a breach of the peace is likely before entering private premises (including a privately hired meeting venue) and if they do not, you can ask officers to leave if you spot them at the meeting.

If officers insist they are simply attending to 'facilitate dialogue', you can remind them that some people may find their presence at the meeting intimidating and an obstacle to speaking. You can also say that if the police want 'dialogue' with your campaign, you would prefer it is in writing. In these circumstances, it is better to have a group of campaign members negotiate the

police's departure from the meeting (to avoid identifying an individual as a 'leader') and to give them a general campaign email address, not a personal one. Remember that you do not have to give you name.

If uniformed intelligence-gathering officers are obviously filming or taking photographs of people arriving for a public meeting, there is nothing to stop you filming or photographing them too. Remember that there is also no law preventing campaigners from covering their faces. Only in limited circumstances where there is an 'Section 60' order in place, allowing searches because of incidents involving serious violence, can officers ask you to remove a mask or covering that they believe is intended to conceal your identity.

Stop and search to gather intelligence

If, as a way to try and gather intelligence, the police use powers to stop and question or search people arriving at or leaving from a meeting, or on their way to and from a protest, remember:

- Although a police officer has powers to stop you at any time and ask you what you are doing, why you're in an area and/or where you're going, you **do not have to answer any questions** an officer asks you.

  You can ask: "am I detained?". If the answer is no then you can walk away.

- You **do not have to give your name or address**, unless you are the driver of a vehicle (when you may also be asked for and must provide your date of birth).

- If a police officer detains you so carry out a search, they must say what they are searching for, the reason they want to search you and why they are legally allowed to search you. They must also provide you with their name and police station and a written receipt.

Your campaign may want to consider holding an introductory 'Know Your Rights' training session for new campaigners. Contact Netpol if this is something you might find helpful.

Organising public protest

Giving notice to the police

There is a right to freedom of assembly, which means that you can arrange and hold protests and public meetings without asking the police for permission. There are some circumstances, however, in which the law states that you must notify the police of your intentions.

If you are organising a rally or other protest at a particular place, there is no legal requirement to tell the police in advance that you are going to do this, or who the organisers are.

If you are organising an event such as a walk around the boundary of a fracking site, it is unlikely you will face any consequences for failing to notify the police beforehand.

If, however, you are planning a march from one place to another, or any form of procession, there is a requirement under section 11 of the Public Order Act 1986 to inform the police at least six days before the procession is going to take place and to provide them with the following details:

- The date when it is intended to hold the procession
- The time when it is due to start
- The proposed route
- The name and address of the person (or one of the persons) proposing to organise it

This makes it easier for the police to manage traffic and disruption, and also to impose conditions on the procession if they think fit. Any conditions are usually applied because a senior police officer "reasonably believes" that a march may "result in serious public disorder, serious damage to property or serious disruption to the life of the community", or lead to "the intimidation of others". They can include restrictions on the route or prohibiting it from entering a particular public place.

It is an offence for organiser of a procession not to give notice to the police, and if convicted they may be fined.

There is no requirement to give notice if it is 'not reasonably practical to do so', which may include a procession with no advance planning and/or no identifiable organisers. In any case, where the organising group is non-hierarchical and has no identifiable leaders, the police often decide against prosecution for a failure to give notice.

Police initiated contact

Prior to (and sometimes after) a protest, demonstration or protest gathering, the police may try to make contact with individuals they have identified as involved or as 'leaders'. This contact may take the form of letters, e-mails or telephone calls, or may include police visits to people's homes.

There is no legal obligation to enter into any dialogue or conversation with the police as a result of these visits.

Officers also have no right to enter your home without your permission.

Some people have been approached by officers from Special Branch or Counter Terrorism units, who have visiting them at home and asked about their involvement in the anti-fracking movement. One, a journalist, was simply making a film about anti-fracking protests. Others have been told that visits are the result of 'concern' about involvement with alleged 'extremists'.

Such visits can be extremely uncomfortable and intimidating for those concerned. You are under no obligation to speak to these officers, you can tell them that you do not want to talk to them and you can ask them to leave and not return. It is quite lawful in such circumstances to record or video these encounters for the purposes of any subsequent complaints.

If you receive a visit, please contact Netpol immediately and in confidence at:

https://netpol.org/campaigns/confidential-contact-form/

Police Liaison Officers

Police Liaison Officers (PLOs, sometimes known as Protest Liaison Officers) have become a regular presence at demonstrations and marches. Anti-fracking campaigners may come across them and can recognise PLOs from the distinctive light blue bibs they wear and their eagerness to 'engage' with protesters' through 'friendly chats'.

PLOs insist that their role is simply to "facilitate peaceful protest" but there is growing evidence that they are central to intelligence-gathering at protests. In 2014 an internal review of the policing of anti-fracking protests in Balcombe confirmed that PLOs played "a pivotal role in the operation" by "interacting with the protest organisers" and as a result, "there was intelligence, including open source, to suggest the protest would escalate".

Netpol strongly advises that you do not engage with Police Liaison Officers at any time.

Even if you think you can 'engage' without giving anything useful away, you are likely to inadvertently divulge information that might seem unimportant to you but can help to build up a profile of your campaign or other activists.

All information gathered – including conversations with PLOs – is shared with an Intelligence 'Bronze Commander' and is also likely to end up on a criminal intelligence database. The police may also keep and share information with the National Domestic Extremism and Disorder Intelligence Unit.

Talk to other campaigners and encourage them to avoid contact with Police Liaison Officers. During a protest, it can become more difficult to ensure this message is conveyed as widely as possible so, beforehand, consider downloading and making our Warning Placards.

These are available at **netpol.org/police-liaison-officers/#placard**