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.

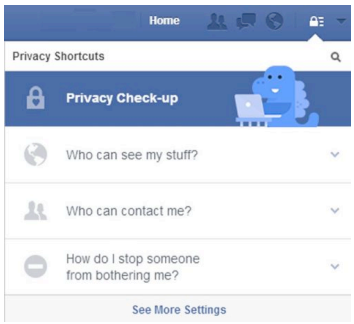
Crabgrass on RiseUp: https://we.riseup.net/
Basecamp: https://basecamp.com/
Pidder: https://www.pidder.de/en/index.html
Trello: https://trello.com/

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.

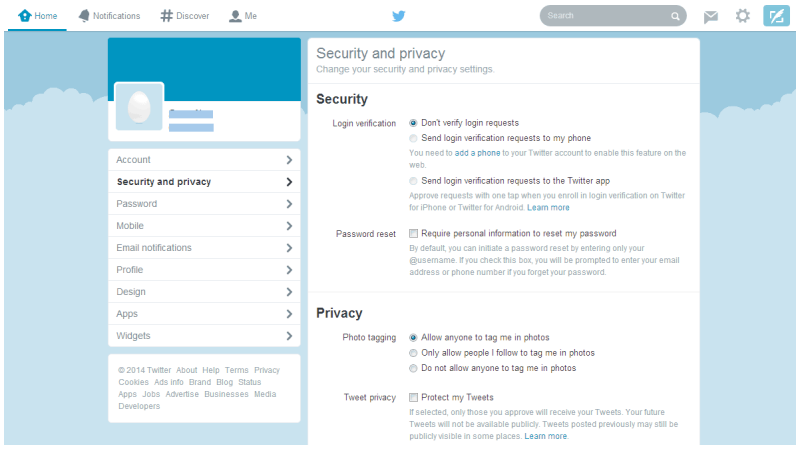
Avoid using location tags in your status updates and prevent others from doing so without your permission by enabling 'Timeline Review'. If you are using Facebook on your phone, turn off GPS location settings

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.