A Guide to Using Mobile Phones Safely

(from freebeagles.org)

Like them or loathe them, the mobile phone is a defining tool of the modern activists. However the benefits they bring in terms of anonymity and mobility have a flip side, of being yet another tool Big Brother can use to keep an eye on us. When the mobile phone becomes indispensable it is a threat to your security and privacy.
But all is not lost, for with a few simple precautions you can use the mobile to it's full potential at only minor inconvenience and little threat to yourself (other than the occasional nuked brain cell).

The technical bit

Mobile phones come in two parts, the actual phone with screen and buttons, etc; and the "SIM card" that associates the hardware with a telephone number. The SIM card is a small strip of plastic with a gold circle on it. It fits in the back of the mobile, usually behind the battery. Each SIM card is unique and identifiable by the mobile number. Appropriate SIM cards can be swapped around.

Most people are paranoid about the SIM card, but the phone itself is also marked with an IMEI number the "International Mobile Equipment Identity" number.

When you make a phone call both your SIM card and IMEI number is broadcast to the mobile phone network.

What makes a mobile phone quite literally mobile, is the presence of mobile phone masts scattered around the country. When your mobile is turned on it and the network constantly check with each other as to where is the nearest mast for it to communicate. In any one area, there may be several masts, so the network and your phone communicate with them all in order to work out which is the best one for you to use.

This is the nasty bit, for using the information provided by these checks, it is not hard to identify roughly where the phone is located. Some estimates claim that this works down to 10 meters, others make more accurate claims. However, the fact that they can locate you to a particular area is damning enough.

Bring in features such as global positioning services (GPS) as now comes available with most phones, whether advertised or not, then your mobile is essentially a homing beacon for those with the power to access this information. This can amount to circumstantial evidence that will stand up in court when tied in with other facts.

Playing safe with mobile phones

That is the downside of mobiles, but none of it is surmountable and there is plenty of fun to be had. In these days of oppression against activists, the mobile allows you to continue to be active and effective while preserving some of your privacy.
The same warnings regarding land-lines being tapped all apply equally to mobile phones. The only difference is that there is not a specific phone to tie you to, and you are not necessarily registered to the number. So, if you can purchase a phone anonymously and use it with a few simple precautions then there is no reason why those trying to invade your privacy will ever be compromised.

Purchasing mobiles anonymously
To ensure anonymity, the law does not forbid you from doing the following tips when buying a mobile phone.

- Make your purchase in a shop away from where you live.

- Try if possible to avoid town centres where there is a greater likelihood that you will be on CCTV. Many small or second hand shops do not have cameras and those that do are unlikely to retain tapes for longer than a few weeks if at all.
- Do not give your real details if asked. Many shop do ask for your details, but not proof of ID, and you are not under any obligation to inform them.
- Go for simple phones without all the extra features now being made available.
- Only pay by cash.
- Do not register the phone – there is no legal obligation to do so.
- Topping up credit
- When setting up the mobile, use pay-as-you-go options only; this is a more expensive solution, but required for anonymity.

Unregistered pay-as-you-go phone calls can be paid for either by using top-up vouchers, or by a swipe card inside a shop. We recommend that you only use top-up vouchers purchased in cash. Using a swipe card to top up within a shop leaves a trail of evidence back to the shop where you could be identified by CCTV or eyewitnesses.

Using personal mobiles safely

By personal we mean mobiles that are going to end up being associated with you. The moment you give out your number to friends and associates it will end up on any network of contacts being monitored by the state. If you are an activist, or your associates are activists, then this will immediately compromise the security of the phone.

- Never say anything on a personal mobile phone you would not wish to have to justify at any point or may incriminate you in any way. Although the mobile may not be used in an action, it use may point to you as being involved and cause you to be investigated.
- Do not take personal mobiles into meetings, and preferably do not even bring them with you. Mobiles are potential listening/tracking devices and should be treated as such.
- If you are on your way to a sensitive meeting, turn your mobile off and remove the battery well before you get to the meeting point, or you may be giving the meeting point away. Even if the meeting is not secret, it is best not to have it present, as you never know what else might be said; besides being very bad etiquette, the safety of others may be put at risk.
- Personal mobiles should be avoided being brought on actions where possible. If you have to bring them, such as for ‘mobile’ demos or if you get separated, take the batteries out until they are needed.
- Another risk area of mobile phones is when people are doing internet activism; there is no point taking a load of security precautions if your mobile phone logs are going to place you as being in the area at the time, or alerting others to the fact that you were in that area so giving them an avenue of investigation.
- We currently recommend against purchasing the higher end of the mobile market where phones have built in camera and other gadgets. Again camera phones hold potential threats to your security, and give them a face to match to your voice. It has not been necessary so far for people to see your face when speaking to you, so it should not matter now. From those concerned with privacy and activism, it is another compromise.
- Never enable GPS or similar such services on your phone if you can help it. Features such as these appear to make life simpler but contain inherent threats to your security.
- SMS / Texting is very useful but also one of the easiest methods to monitor. It is known that scanning software is available for monitoring them, but tends to be only in the hands of security services as opposed to the police. However, if a hacker was to break into a mobile phone

operator's databases then the chances are that they too could monitor in what ever fashion all the information passing through, and pick up on sensitive details that you are sending via text. Make sure you delete your text messages and never write anything you would be unable to defend in court.

Finally, mobiles can also be used to confuse. Say one mobile phone was used in an action and you have been accused of using that phone at that time. A possible defence is to say that it could not have been you as if they were to look at the logs of your actual phone, that everyone knows is yours, then it was in a different place altogether. In other words, the tracking capability of mobile phones can also be used to provide alibis, especially if calls were made from the phone at the time of the alleged offence.

Mobile phones and activism

There are two scenarios to consider here. The first is where mobiles are used to facilitate the action, but not the action itself. The second is when the mobile is an intrinsic element of the action.

Facilitating actions

In the first case, this could be when an action needs to be co-ordinated. If there is a lot of risk attached to this, it is worth investing in a set of mobiles to be used specifically for it. Second hand mobiles may be useful in this case, as the chances are that after the action the mobiles will have to be discarded – just do not buy them off friends! The reason behind this, is that if you have a set of mobiles that have never been associated with your network of contacts and friends, it is impossible to connect them back to you.

This means you can set up an anonymous network that will not draw attention from the various authorities listening in. Avoid bringing attention to it by not saying anything explicit on it, but using code. Keep the batteries out of the mobile until they are required, and when testing that all is working fine, chose an area free of CCTV. Testing that the mobiles work and that everyone can use them and has the relevant numbers is important.

We also recommend that you burn the packaging that comes with the phones. The mobiles should be disposed of afterward, ideally by burning. It is no longer enough just to destroy the SIM cards and reuse them.

Mobile phones for activism

As noted, mobile phones are a very useful tool. There are many situations whereby you want to contact another telephone number anonymously. So some guidelines:

Follow the above guidelines for purchasing a mobile phone anonymously.

- Do not ring your friends or contacts from the mobile; if you have to do this, then get rid of the mobile immediately afterwards as it has been compromised.
- Keep the battery out of the mobile when not in use.
- Keep the SIM card out of the mobile when not in use; preferably store them separately.
- To make the phone call, travel to the area avoiding CCTV as much as possible. A quick bike ride into the countryside or a suburban bus-shelter usually does the trick.
- Try to avoid spending longer than 30 minutes in one area. Make use of the fact that the phone allows you to be mobile.
- Do not slip into a pattern of using the mobile at a certain time or certain place or it will end up as being little better than using it at home.
- Use 141, but remember that it will not work for a lot of targets receiving a large amount of actions against them. On the whole, 141 is not as useful as it once was for privacy issues, though it still serves some purposes.

- Do not answer calls to the phone and ignore any messages they leave on your answering service; as tempting as it is to hear their reactions, do not play into their hands.

Depending on how much you use the phone, what you say on it and how your target reacts, you need to consider changing the SIM card after a length of time. The heavier the use, or the more legally risky stuff you say on it (or not as maybe the case) will require regular changes of the SIM card and even of the phone itself.

Targets react to phones in several ways. They can end up blocking that number altogether, in which it will be useless against that target. However, as most people involved in activism have more than one target, it is simply a matter of moving onto the next target that has not blocked it. In many cases, the block may only happen for one number in a company, and not others. As it is likely that it is only the SIM card that has been blocked, you only need to change this in order to be able to contact that telephone number again.

Some companies simply send out a warning that your calls have been logged and the police informed. We know of one situation where police did turn up within the hour, though this appears to be the exception and only followed on after heavy use of the phone in the same area over a few weeks. To play it safe, do not reply to the message, take the battery out at once and leave the area, preferably stashing the phone somewhere on the way. If you have taken all the above precautions, then there is little anyone can do to identify you.

What the law says

Stolen and reprogramming mobiles
Stolen mobile phones can be disabled across all networks as the different operators and the government are now co-operating on this issue. A side effect of this is that phones used as part of activism now also have the potential to be blocked, though we have not been made aware of this having happened. This blocking is done to the actual phone (through the IMEI number) and not just to the SIM card. For more information on the UK initiative on stolen mobiles see www.immobilise.com.
It is possible to re-programme the IMEI number in a mobile, however this is an offence in the UK with a maximum 5 years imprisonment.

Repeat ringing
Ringing another telephone number constantly may amount to harassment, though it is not clear what the legal situation is regarding allowing it to ring once before cancelling the call. This is a tactic thought to be favoured by some activists who do it repeatedly over a length of time for effectiveness. This is not a course of action we recommend as it could be illegal, since it may amount to harassment or an offence under the Telecommunications Act 1984.

Future developments

Mobile phone manufactures and software companies are working very closely together to develop new services for mobiles. There is a natural trend to turn to the mobile into a miniature computer. Unfortunately, these come with a lot of security risks.

There have also been a number of stories about commercial systems now being able to use mobile phones and the internet to monitor people. This is being done under the guise of monitoring lazy workers or protecting children. However, the obvious threat to civil liberties is there.

So far, in order for these commercial services to work, a text message is sent to your mobile from the tracking service, and you have to reply (that is give your assent) to activate it. It should be standard policy on your part, never to reply to unsolicited texts or texts from numbers you do not recognize. If you get one from one of these services, then simply ignore it. It only becomes a threat if you reply to it.

The risk is, if your house is broken into by whatever authorities or company are watching you, and they do the reply for you (it would be relatively simple to arrange to have a text message sent at the appropriate time, and subsequently delete it, in which case you would be blissfully unaware). The simple solution is to take the SIM card out when not using it, especially at night, and store it separately, as we have already suggested you do with phones being use for activism.

Note: there is a lot of information on how mobiles can be used to spy on you at http://www.spywareinfo.com/articles/cell_phones/, but note that this is principally for the US situation. How it applies to other countries is not clear.

Conclusion

It is our opinion that mobile phones are great for activists and that their potential has not been fully realised yet. However, like all technology they carry risks for privacy and security, though nothing that cannot be dealt with by taking some simple precautions. Yes it can be a pain to follow them through all the time, but think about what you are trying to achieve in the long run. Like all security, the more you practise it, the more it becomes second nature as you practise it automatically.

The phone is a staple for modern society, companies and people simply cannot function without them. This makes the phone a fantastically useful target for the activist. So spend a little time and money getting it right and you can have hours upon hours of useful fun…

This article is for information purposes only; its aim is to let people to know their full rights under UK law. Nothing on these pages is absolute as the law is always changing; if in doubt contact a trusted solicitor for further advice. We do not encourage you to break the law.

If you see any errors, or we have missed any changes to the legal situation please contact us as soon as possible, at info@freebeagles.org, as wrong information can prove costly to people's freedom.