London Calling:

a cellphone and internet security primer for the criminally-minded anarchist

j/k enterprises, 2011
love for our friends in lockup
hate for those who put them there

wrap it so they can't tap it: security as harm reduction

THERE'S A FAIR AMOUNT of skepticism, mixed messages, and general confusion in criminally-minded political scenes these days about what, exactly, constitutes good security in relation to technology. We want to try to clarify a few things, and help you to protect yourself against surveillance. As when having sex, there's no way to be perfectly safe while using technology, but we can at least practice harm reduction. This zine is not about security culture, an idea about which we have strong and conflicting feelings, although there's some connection between that concept and technological surveillance in relation to social networking. The only overall notion about security we'd like to convey is risk management: knowing the risks, weighing them against convenience and need, and making an informed decision. Likewise, the laws about surveillance are also largely outside the scope of this zine--it matters more to us what the cops can do than what they are legally allowed to do. Even if they can't use the information they gather in court, it can aid their investigations.

Mulder? It's me: cops and phones

WE WANT TO EMPHASIZE how *easy* it is for the bad guys to get access to your phone, calls, and phone records. There doesn't have to be a guy with headphones on, listening to your live conversations from a van parked down the street (although that still works, too; cellphones send out radio signals that are easy to intercept); nowadays they have an extensive surveillance network called DCSNet that does all the work for them.

> "The FBI has quietly built a sophisticated, point-and-click surveillance system that performs instant wiretaps on almost any communications device, according to nearly a thousand pages of restricted documents newly released under the Freedom of Information Act. The surveillance system, called DCSNet, for Digital Collection System Network, connects FBI wiretapping rooms to switches controlled by traditional land-line operators, internet-telephony providers and cellular companies. It is far more intricately woven into the nation's telecom infrastructure than observers suspected. It's a "comprehensive wiretap system that intercepts wire-line phones, cellular phones, SMS and push-to-talk systems," says Steven Bellovin, a Columbia University computer science professor and longtime surveillance expert...

DCSNet is a suite of software that collects, sifts and stores phone numbers, phone calls and text messages. The system directly connects FBI wiretapping outposts around the country to a far-reaching private communications network. The $10 million DCS-3000 client, also known as Red Hook, handles pen-registers and trap-and-traces, a type of surveillance that collects signaling information -- primarily the numbers dialed from a telephone -- but no communications content. (Pen registers record outgoing calls; trap-and-traces record incoming calls.) DCS-6000, known as Digital Storm, captures and collects the content of phone calls and text messages for full wiretap orders. A third, classified system, called DCS-5000, is used for wiretaps targeting spies or terrorists. Together, the surveillance systems let FBI agents play back recordings even as they are being captured (like TiVo), create master wiretap files, send digital recordings to translators, track the rough location of targets in real time using cell-tower information, and even stream intercepts outward to mobile surveillance vans. FBI wiretapping rooms in field offices and undercover locations around the country are connected through a private, encrypted backbone that is separated from the internet. Sprint runs it on the government's behalf. The network allows an FBI agent in New York, for example, to remotely set up a wiretap on a cell phone based in Sacramento, California, and immediately learn the phone's location, then begin receiving conversations, text messages and voicemail pass codes in New York. With a few keystrokes, the agent can route the recordings to language specialists for translation. The numbers dialed are automatically sent to FBI analysts trained to interpret phone-call patterns, and are transferred nightly, by external storage devices, to the bureau's Telephone Application Database, where they're subjected to a type of data mining called link analysis. (1)

Alternately, they can have your phone record the conversations you have over it and transmit the recordings to them (2). Easiest of all is getting and using the records of who you called and when--this has been done and used in countless activist trials. We must recently saw it cited (3) in Marie Mason's sentencing hearing to suggest that she is/was a leader in the anarchist scene, receiving reports and giving commands after her arrest. This notion has put her under intense scrutiny as a prisoner; they've used it as a pretext to try to cut her off from comrades.

P.S. Not only are text messages as vulnerable to radio interception as calls, they're not protected by the Wiretap Act--so cops don't even need a court order to be able to intercept them. (4)

where in the world is the ALF?

Cell phones work by bouncing signals off cellphone towers. Your phone sends a signal to a tower about once every seven seconds. Cell phone companies keep this information on file for a few months to a couple of years. (5) The FBI routinely uses this information to arrest and convict people; for example, William Viehl was convicted of liberating mink largely because of cell phone records that placed him near the farm during the liberation. (6) (His car key was also found at the scene... ouch.) In short, take your batteries out before, during and after any journeys to the scene of your crime, your associates, house, etc. for maximum safety.

You can also consider buying a less traceable prepaid phone, although if you're caught with it that won't help you much. Remember to use only cash and not give an ID when you buy it, don't use your old SIM card (both SIM cards and phone hardware transmit an identifying signal), etc. Even so, are you sure that your friends won't save your number under your real name, or a fake name that's ever been linked to your legal identity? Are you sure no one will call you by your real name over the phone?

these are not the droids you're looking for

There's some hope, though it's only a matter of time until every new, safer way to handle your communication doesn't work anymore:

Android phones are a partial solution to phone security for now. You can make completely secure calls, text messages, run the entire internet through TOR (which masks your activity), and, with certain phones, encrypt everything. Check these resources for more. (7)

when they take your cellphone, how's it gonna come?

From the EFF's excellent guide to surveillance, cited earlier (4):

> "If you are arrested, the officers are going to seize all the property on your person before you are taken to jail. If you have a cell phone or a laptop, they will take that too. If you are sitting near a cell phone or laptop, they may take those as well. The SITA doctrine may allow police to search the data. It many also allow copying for later search, though this is well beyond what the SITA doctrine's original justification would allow. You can and should password-protect your devices to prevent this potentially unconstitutional privacy invasion. But for much stronger protection, consider protecting your data with file and data encryption. Prudent arresting officers will simply secure the devices while they get a warrant. There's nothing you can do to prevent that. Do not try to convince the officers to leave your phone or laptop behind by disavowing ownership. Lying to a police officer can be a crime. Also, prosecutors may use your statements against you later to argue that you do not have the right to challenge even an illegal search or seizure of the device, while still being able to introduce information stored on the device against you."

However, the search incident to arrest (SITA) doctrine they're referring to here does not extend to, say, the trunk of the car you were arrested in; they need a separate search warrant for that (unless they impound the car). We mention this only to show that it isn't entirely hopeless; an encrypted laptop locked in the trunk of your car or inside a hidden safe in your basement will be considerably more frustrating to the cops than not, and might entirely escape scrutiny.

zombie robots: remote access

WHILE EVERYONE KNOWS AT least a little about wiretaps (though not enough; check the EFF's incredibly useful guide (4) for more info), people still seem skeptical about cellphones being used as microphones. The idea of taking your batteries out of your cellphones has been around for awhile, but, five years later, some people still seem skeptical. Here's a cold hard truth bomb for you types:

> "The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations.
>
> The technique is called a "roving bug," and was approved by top U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance techniques such as tailing a suspect or wiretapping him. Nextel cell phones owned by two alleged mobsters, John Ardito and his attorney Peter Peluso, were used by the FBI to listen in on nearby conversations. The FBI views Ardito as one of the most powerful men in the Genovese family, a major part of the national Mafia.
>
> The surveillance technique came to light in an opinion published this week by U.S. District Judge Lewis Kaplan. He ruled that the "roving bug" was legal because federal wiretapping law is broad enough to permit eavesdropping even of conversations that take place near a suspect's cell phone.
>
> Kaplan's opinion said that the eavesdropping technique "functioned whether the phone was powered on or off." Some handsets can't be fully powered down without removing the battery; for instance, some Nokia models will wake up when turned off if an alarm is set.

> While the Genovese crime family prosecution appears to be the first time a remote-eavesdropping mechanism has been used in a criminal case, the technique has been discussed in security circles for years...
>
> Nextel and Samsung handsets and the Motorola Razr are especially vulnerable to software downloads that activate their microphones, said James Atkinson, a counter-surveillance consultant who has worked closely with government agencies. "They can be remotely accessed and made to transmit room audio all the time," he said. "You can do that without having physical access to the phone."
>
> Because modern handsets are miniature computers, downloaded software could modify the usual interface that always displays when a call is in progress. The spyware could then place a call to the FBI and activate the microphone--all without the owner knowing it happened. (8)

There you go, documentation. We could only find this one documented case so far, but that doesn't mean that it doesn't happen more frequently. Several articles we saw, including one by the U.S. Commerce Office (9) and one by the BBC (10), recommend that government officials and company executives take their batteries out when discussing sensitive matters. Is it fishy when ten activists' (or Mafia bosses') cellphones all blink out at once? Maybe! Feel free to leave your cellphones intact and go for a walk without them instead.

There are many legal ways to remotely access both Windows and Mac computers, using commonly available programs. They can look through your files, monitor your activity, turn on your microphone, record video or take photos of you with your webcam (11). There are also keystroke loggers, programs that record everything you type and transmit it off to someone. Someone can park outside your house and record your unencrypted internet communication, or break the encryption, given enough time. This is fairly well-known; the best way to avoid it is to use a public computer, at an internet cafe or library, while paying in cash or using a guest pass.

not all trolls do it for the lulz: internet surveillance

IT'S FAIRLY WELL-KNOWN by now: what you post on a social networking site can be used against you in court. It happened to Marie Mason (for listing Rod Coronado as a hero on her MySpace (3)); it happened to Rod Coronado (for adding Mike Roselle on Facebook (12)); it happened to kids during the recent London riots (for posting vaguely pro-riot statuses on Facebook (13)); and in hundreds of less obviously-political cases. Every one of these intangible posts resulted in very real jail time. This obviously makes social networking sites goldmines for law enforcement, but it's only the tip of the iceberg. Think about it: Facebook literally provides the FBI with a map of anarchist social relationships, hundreds of anarchists and their activities, degrees of closeness to each other, and so on. Even if you use a fake name, don't

join anarchist groups, don't get invites to anarchist events and never post about politics, a preliminary study (14) shows that researchers can easily determine if someone is gay or Christian by surveying their Facebook friends' interests: if most of your friends are Christian, you probably are too. The same goes for anarchists. Besides, if you ever sign into Facebook from your own computer, they have a record of your IP address having done so, and they will happily turn it over to the police (they handle such requests--hundreds a week--through the email address subpoena@facebook.com. So intuitive!) Think about it: do you trust everyone you're friends with on Facebook to refuse to talk to the cops? Social networking connections are a great basis for conspiracy charges, too.

Even if you don't use social networking sites, you probably use email. Virtually all email providers will surrender copies of your emails and the relevant IP addresses to law enforcement--in fact, a court ruling from 2009 permits the police to read your email without even a warrant. (15) riseup.net, an anarchist-run email service, has pledged to resist any such attempt by law enforcement, but they are the only service we are aware of that makes such resistance their policy. Their policy reads, in part:

> "We strive to keep our mail as secure and private as we can. We do not log your IP address. (Most services keep detailed records of every machine which connects to the servers. We keep only information which cannot be used to uniquely identify your machine). All your data, including your mail, is stored by riseup.net in encrypted form. We work hard to keep our servers secure and well defended against any malicious attack. We do not share any of our user data with anyone. We will actively fight any attempt to subpoena or otherwise acquire any user information or logs. We will not read, search, or process any of your incoming or outgoing mail other than by automatic means to protect you from viruses and spam or when directed to do so by you when troubleshooting. (16)"

We strongly recommend using a riseup account for any kind of personal communication, although we still don't recommend sending anything sketchy over email; it's just a better bet, and at least keeps your data from being mined as easily. There's also an encrypted instant-message service (17).

We've mentioned data mining before in reference to the police, but it's also done by private companies (who are always happy to cooperate with the authorities.) Google (18) is an easy example: do your search results and advertisements seem creepily pertinent? It's because Google is keeping track of everything you search for, all the sites you visit; if you use Gmail, it also notices the words you send or receive in your emails; if you use Google Voice, it even records the notable things about your voice and, given enough data, can identify your voice in other contexts. Not searching through Google or having any Google accounts might be slightly helpful, but the company will still track everything your IP address does on any affiliate site of theirs. And Google is just the best at this--most widely-known alternatives track you similarly.

As we said earlier, public computers are your best option, security-wise--remember to not sign into any accounts linked to your home IP or name, and to not use ID when signing up for the computer (such as a library card, or paying with a credit card at an internet cafe.) You can also use tools like TOR to mask your activity, VPNs to encrypt it, or PGP/GPG to encrypt your messages; other computer security options to look into include secure deletion (deleting your files the ordinary way doesn't actually remove information from your computer or phone, only strips off the file name), and encrypting your hard drive.

repression

All of the surveillance tools we've discussed in this zine (and more) were used against protestors and rebels during the Arab Spring uprisings. For example, tools used in Bahrain:

> "Monitoring centers, as the systems are called, are sold around the globe by these companies and their competitors... They form the heart of so-called lawful interception surveillance systems. The equipment is marketed largely to law enforcement agencies tracking terrorists and other criminals. The toolbox allows more than the interception of phone calls, e-mails, text messages and Voice Over Internet Protocol calls such as those made using Skype. Some products can also secretly activate laptop webcams or microphones on mobile devices. They can change the contents of written communications in mid-transmission, use voice recognition to scan phone networks, and pinpoint people's locations through their mobile phones. The monitoring systems can scan communications for key words or recognize voices and then feed the data and recordings to operators at government agencies. (19)"

Many people were singled out for reprisals--detainment, torture, murder and rape--by authorities using information gathered from this surveillance of cellphone and internet use. While laws in many

countries prohibit this kind of surveillance, laws are often broken or suspended by governments seeking to reconsolidate their control... and Western companies are largely responsible for producing these technologies (Cisco is complicit in China's repression of internet freedom, for example (20)).

Infamously, cellphone signals were blocked at a BART station recently in anticipation of a protest against BART police, who had murdered someone. (21) The British government is promising to block Twitter and Blackberries during future social unrest (22), and of course Mubarak did this in Eygpt towards the end. In short, the internet, social networking, and mobile access are often great tools for us, but they do not belong to us. We need the army of black hat hackers working busily to undermine the government and corporate control of the internet--but until they win completely, we can't rely solely on it. Too, some people think that social media tends to turn people into armchair revolutionaries, that it satiates those who would otherwise be in the streets. (23) We can't lose our ability to work face to face, directly, to plan in unmonitorable ways; to strike quickly, secretly, and to get away with it; to know when it's worth it to organize via Twitter (was Pittsburgh (24) worth it? discuss); to know when the only kind of security necessary is a t-shirt wrapped around your face so that CCTV can't recognize you, and you become a target that isn't worth it in a sea of other looting bodies. We have to be able to distinguish between these situations, rather than settling into a static stance.

good old fashioned lover spy: friends n' bedrooms

Don't forget: while the cops can spy on you in all kinds of high-tech ways, they're often too overworked or bogged down in bureaucracy to get to it--but the easiest kind of intelligence is also the oldest: gossip. No matter how safe you're being technically, your acquaintances, exes, even your good friends can always rat you out. No matter how advanced your encryption is, the FBI can always put a bug in your lampshade. Don't let taking more advanced security measures lull you into forgetting the most basic. We don't want you to be paranoid, but we do want you to be discreet, know your risks, and be okay with the consequences of your actions beforehand.

(re)sources

1. http://www.wired.com/politics/security/news/2007/08/wiretap
A very informative article on DCSNet.
2. http://mobileactive.org/howtos/mobile-surveillance-primer
Discussion of cellphone security risks, suggestions for making phone use safer. UK-focused.
3. http://supportmarie.files.wordpress.com/2011/03/mason-sentencing-transcript.pdf
Marie Mason's sentencing transcript.
4. https://ssd.eff.org/
This entire site is an excellent resource for information on American government surveillance and protecting yourself.
5. http://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r=3&src=me&ref=general
An article about German cellphone location tracking.
6.http://www.voiceofthevoiceless.org/activist-sentenced-to-two-years-for-alf-mink-liberation/
Information about William Viehl's conviction (based partially on his cellphone being tracked near the mink farm.)
7. http://guardianproject.info and http://www.whispersys.com/
Information on making Android phones safer.
8. http://news.cnet.com/2100-1029-6140191.html
An article on Mafia bosses being recorded by remote activation of their cellphones.

9. http://www.wrc.noaa.gov/wrso/security_guide/cellular.htm#Cellular%20Phones
The US Commerce Office's guide to cellphone security.
10. http://news.bbc.co.uk/2/hi/uk_news/magazine/3522137.stm
The BBC on surveillance risks for political and business leaders.
11. http://news.cnet.com/8301-19518_3-10457737-238.html
An article about remote webcam activation.
12. http://missoulanews.bigskypress.com/images/blogimages/2010/08/24/1282683297-coronado-petition_for_warrant_or_summons.pdf
The court document on sending Rod Coranado back to jail for adding Mike Roselle on Facebook.
13.http://www.guardian.co.uk/uk/2011/aug/16/uk-riots-four-years-disorder-facebook?INTCMP=ILCNETTXT3487
An article on the kids who were sent to jail for four years for posting pro-riot Facebook statuses.
14. http://www.inquisitr.com/38594/closeted-your-facebook-friends-could-out-you/
A post about the preliminary study that showed it was easy to determine your sexual orientation from your Facebook friends alone.
15. http://online.wsj.com/public/resources/documents/062309mosman.pdf
The court ruling that confirms the police's right to read emails without a warrant.
16. https://help.riseup.net/en/about-us
Riseup's policy of keeping your data secure and resisting law enforcement.
17. https://help.riseup.net/en/otr#introduction-to-otr
An introduction to Off The Record and Pidgin, an encrypted instant message service.
18. http://www.spiegel.de/international/germany/0,1518,587546,00.html
Der Spiegel's article on Google's data mining practices.
19. http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html
Information about how Western companies' surveillance technology

was used to repress participants in Arab Spring.
20. https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-human-rights-china-part-1
Cisco's role in aiding internet censorship in China.
21. http://news.cnet.com/8301-27080_3-20091822-245/s.f-subway-muzzles-cell-service-during-protest/?part=rss&subj=news&tag=2547-1_3-0-20
Article on BART's disruption of cellphone service, intended to prevent a protest.
22. http://www.guardian.co.uk/uk/2011/aug/11/cameron-call-social-media-clampdown
David Cameron promises to cut off access to Facebook, Twitter, and the Blackberry network in future social unrest.
23. http://theconversation.edu.au/dictatorship-101-killing-the-internet-plays-into-the-hands-of-revolutionaries-3254
Discussion of a paper that suggests the internet tends to pacify revolutionaries.
24. http://www.post-gazette.com/pg/09278/1003126-53.stm
Two people were arrested for tweeting police activities during the G20 in Pittsburgh.

Not directly referenced:
http://www.zahrasparadise.com/lang/en/archives/76
Zahra's Paradise, by Amir and Khalil; a webcomic about internet resistance and repression in Iran, as well as being a general account of the 2009 uprisings. Also available in book form.
http://www.thoughtcrime.org/software.html
Moxie Marlinspike's software: some anonymizing, some oriented towards attack.
https://we.riseup.net/
Crabgrass, a more secure social networking site, run by riseup.net. In beta testing.
http://www.eff.org/
The Electronic Freedom Foundation: like the ACLU for the Internet.
http://craphound.com/littlebrother/download/
Cory Doctorow's YA novel *Little Brother*, free for download. A novel about youth resistance to Homeland Security surveillance measures.

ten take-aways:

1. Act as if absolutely no phone conversation you ever have or text message you exchange on a phone that is clearly yours is remotely private.

2. Don't say anything implicating around a cellphone or computer. Face to face and outdoors is the only way to be sure that the person you're talking to you--and your own future carelessness--are your only security concerns.

3. Know that surrounding data is also collected by the cops--who you talk to, gossip that indicates the structure of your scene, etc--and keep that in mind while having monitorable conversations.

4. Batteries out on your way to and from committing your crime, scouting for it, meeting up with your associates--any time you don't want your location to be easily placeable--if you can't just leave your phone at home.

5. Email is not secure, but riseup-to-riseup is your best bet for non-incriminating personal conversation.

6. Your IP address is being logged constantly by various websites--using a public computer without showing ID or signing into anything is safest.

7. If you steal something electronic, make sure to know beforehand how to deactivate any tracking mechanisms it may have.

8. If your political resistance depends on social networking, know that it can be crippled in an instant.

9. It's not necessary and may be counter-productive to abandon higher technology as an anarchist, but think through your interactions with it carefully.

10. Don't let taking the highest precautions make you forget to take the most basic.