Never Turn Off the Phone

a new approach to security culture

Anonymous

Contents

[ed. – First hosted by the Russian anarchist site a2day.net; see compiled international documentation of actual surveillance operations against anarchists at earsandeyes.noblogs.org]

In the 80s, an anarchist who wanted, for example, to burn some building, developed their plan and at the same time checked that there were no listening devices in their house. In the late 90s, the same anarchist turned off the phone and used encrypted traffic on the Internet. In the 2020s, we need to reconsider our strategy: intelligence gathering has improved and we must also take this into account.

To begin with, let's see how big data analysis is used. To do this, we need to talk about 3 things: metadata, templates and networks. It seems boring and difficult, but I am not a technician, and I will not bore you with technical language, I will make it as simple as possible.

Metadata

In the context of online activity, "content" means "the message you sent", and "metadata" means "everything except the content". So, for example, if you send a text about lunch to your friend, the content may be "Let's go have lunch", and the metadata may be "Message sent 01/04/2018 11.32 from 0478239055 to 079726823 using Signal".

This information is recorded by your phone, even if the application encrypts your actual message. Your metadata is very poorly protected by technology and very poorly protected by law. No matter what country you are in, the majority of your metadata is freely available to secret services, regardless of whether you are suspected of something or not.

Templates

Whether you realize this or not, your metadata has a template. If you have daily work, you may have a very consistent pattern; if there is no such work, your template may be more flexible, but you still have a template. If someone wants to know the rhythm of your day, they can do it very easily, because your template is in metadata.

For example: Maybe you use Wi-Fi in your favorite bar on most Sunday nights until midnight, you wake up around 10 am and check your Signal, you use your public transport card to get to class every Monday afternoon, and you spend an average of 1 hour per Tumblr twice a day. All this is part of your template.

Network

You have an online network. Your friends on Facebook, the people in your phone's address book, the dropbox you are sharing with your colleagues, everyone who bought online tickets for the same punk gig that you attended, people using the same WiFi points as you. Take your networks, combine them with the networks of other people, and the clusters will manifest themselves. Your working community, your family, your activist scene, etc.

If you are in the anarchist community, it is likely to be quite obvious from all of your small network connections, such as visiting one band and knowing the same people as other anarchists. Even if you have never clicked on an anarchist Facebook page or didn't click the go button on the anarchist Facebook event, your network is hard to hide.

Now, let's say you committed a crime, one that would lead to a serious investigation.

Suppose that on Sunday at 3 am, you and your friends go out and burn the house of the Nazis. (Of course, I would never advise any of you to do something like this.) Obviously, the anarchists did it, but there are no other clues. You are using a traditional security culture: you burn records, you try not to communicate your plans near technology and you leave no physical traces.

But since you committed a crime that night, your metadata will be very different from your usual rhythm: you stay in your usual bar until 2 am to wait for your friends, you will not wake up at 10 am and check your Signal or you will Tumblr only for an hour of the day. You do not go to class. Your metadata template is very different from your regular template. Your friends' metadata models are different too. If one of you is clumsy, they can generate a super-suspicious metadata signal, for example, the phone turns off at 2.30 at night and is activated at 4 am. You wouldn't be the first.

If I wanted to solve this crime using data analysis, then I would do the following:

- allow a piece of software to analyze the patterns of the local anarchist scene to identify the 300 people most associated with the anarchic scene;
- allow the second piece of software to analyze the metadata samples of these 300 people in recent months and identify the biggest metadata changes on Sunday evening, as well as any very suspicious metadata activity;
- exclude variations of the pattern with an obvious reason or an obvious alibi (people who are on holiday, people who are in hospital, people who have lost their job, etc.);
- conduct a more in-depth study of those who remained.

That's right, from the huge number of people I could not listen to at the same time, I can quickly identify a few in order to closely monitor them. So I could find and catch you.

And Now What?

If a traditional security culture will not protect us like before, how do we adapt? Well, I have no answers, but for a start I would say: know your network + know your template.

In the case of the example above: leave the bar at midnight, go back home and put the phone on the bedside table. Check the apps you usually check before bedtime and set the alarm for 10 am. Return to the bar without a phone. Wake up at 10 in the morning and check your Signal. Drag yourself to class or ask a friend to travel with your travel card and do not use technology in your home while a friend travels with your travel card to class. Stick to your template. Never turn off the phone.

You can also manipulate your network, but it is much more difficult to do. Do not use the smartphone in general and abandon all social activity on the Internet – this requires serious motivation. Knowing your data template and making sure that it looks ordinary is much easier.

Some of the old rules will still apply: do not talk about crime around devices with microphones, do not brag after successful actions, etc. Other rules, such as "turning off the phone when planning illegal actions", need to be changed because their metadata looks too unusual. No one else disconnects their phone. We look suspicious when we do this.

This is just one idea on how we could update our security culture. Perhaps there are other people with different, better ideas about updating it. If we start a conversation, we can get somewhere.[1]

Finally: We Need to Continue to Adapt

As technology changes, more information emerges, including data that we have very little control over. Smart-TV and advertising in public places that listen to every word that we speak, and the tone of our voice when we speak, these are examples. Currently, data analysis projects use license plate reading software to compare vehicle traffic patterns. It says a lot that they may soon be ready to do the same with facial recognition, after which the presence of our face in the public space will become part of our metadata. Additional information means more accurate data analysis. Our metadata may soon be too extensive, which is too difficult to fully reflect and mirror. This means that we will need to adapt our counter measures if we want to hide something.

How do we keep all this under the radar? I don't know. But let's try to understand this shit. These are some first thoughts on how a security culture should look like in an era of modern analysis of large data sets, and I would be very happy to receive additions from comrades who have thoughts on this.

[1] ed. – " "Security culture" should always be understood as a strategic race against enclosure rather than a technical elaboration of rules of behavior, because the latter is a practice based on the imperative of keeping people out of prison. In individual cases, this is perfectly sensible. In the big picture, perfectly absurd. Wherever there is effective struggle, the State will make arrests, whether or not they can find the people responsible for specific crimes. The proposition of keeping people out of prison is, in the long run, conservative and idiotic. Notwithstanding, by perfecting techniques of security, we force the State to fall back on collective rather than individualized forms of punishment. If they cannot find the specific criminals responsible for an attack, they must attack the community of struggle and arrest scapegoats singled out for clearly political reasons, which belies the narrative of democratic peace, destroys the discourse of criminality and the alibi of the justice system, and reveals the fundamentally collective nature of all struggle. Partisan movements, urban guerrilla groups, and Native land struggles have all produced technical manuals focused on counter-surveillance that rebels and insurgents today can make use of to obstruct State efforts to gather intelligence. The urban guerrillas in particular communicate a mythology of clandestinity which requires the reader to separate the technical knowledge from the strategic. The real trick is not to professionalize these techniques but to generalize them among a larger community. A broadly shared suspicion of communications technology, academics, journalists, and police, in the hands of an entire community, will be far more effective at blocking State intelligence-gathering than a sophisticated array of counter-surveillance techniques in the hands of one affinity group; but the one need not and should not exclude the other" (Here… at the Center of a World in Revolt).

Anonymous
Never Turn Off the Phone
a new approach to security culture

Printed in Return Fire vol.6 chap.4 (summer 2022). PDFs of Return Fire and related publications can be read, downloaded and printed by visiting returnfire.noblogs.org or emailing returnfire@riseup.net

theanarchistlibrary.org