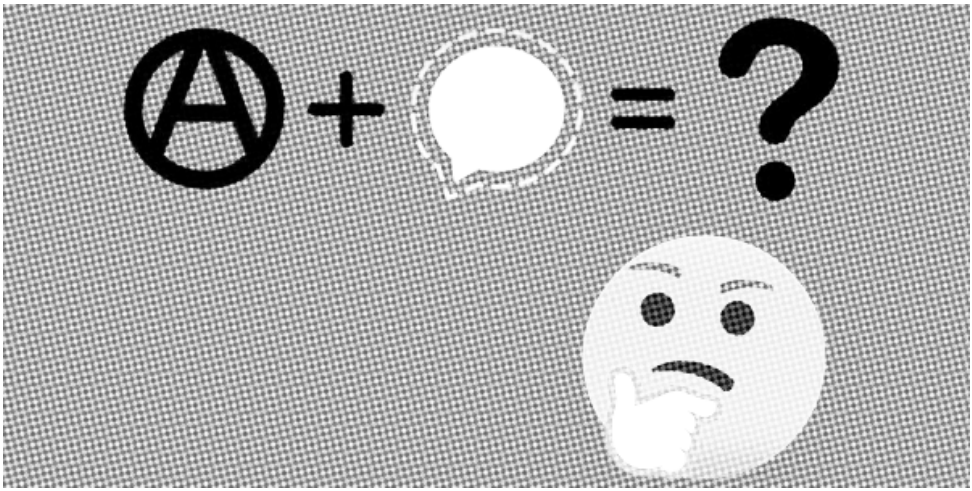
Signal Fails



Signal Fails

Original text in English
2019
north-shore.info/2019/06/02/signal-fails

Layout
No Trace Project
notrace.how/resources/#signal-fails

Contents

Introduction

Signal[1] is an encrypted messaging service that has been around in different forms for about 10 years. Since then, I have seen the software widely adopted by anarchist networks across Canada and the United States. More and more, for better and for worse, our interpersonal and group conversations have moved onto the Signal platform, to the extent that it has become the dominant way anarchists communicate with each other on this continent, with very little public debate about the implications.

Signal is just a smartphone app. The actual paradigm shift that's happening is to a life increasingly mediated by smartphone screens and social media. It only took a few short years for smartphones to become mandatory for anyone who wants friends or needs work, outside of a few scattered pockets. Until recently, the anarchist subculture was one of those pockets, where you could refuse to carry a smartphone and still socially exist. Now I'm less sure, and that's fucking depressing. So I'm going to stubbornly insist throughout this text that there is no substitute for real-world face-to-face relationships, with all the richness and complexity of body language, emotion, and physical context, and they continue to be the most secure way to have a private conversation. So please, let's leave our phones at home, meet up in a street or forest, conspire together, make some music, build some shit, break some shit, and nurture offline living together. I think this is way more important than using Signal correctly.

The idea for this zine came about a year ago, when I was visiting friends in another city and joking about the ways Signal conversations back home turn into trainwrecks. The patterns were immediately recognized, and I started to realize that this conversation was happening in a lot of places. When I started asking around, everyone had complaints and opinions, but very few shared practices had emerged. So I came up with a list of questions and circulated them. I was pleasantly surprised to receive more than a dozen detailed responses, which combined with several informal conversations, inform the majority of this text[2].

[1] https://signal.org

[2] Big thanks to everyone who submitted! I stole a lot of your ideas.

I'm not an expert—I haven't studied cryptography and I don't know how to code. I'm an anarchist with an interest in holistic security, and a skeptical relationship with technology. My goal with this piece is to reflect on how Signal has become so central to anarchist communication in our context, appraise the implications on both our collective security and social organization, and advance a few preliminary proposals towards developing shared practices.

A Brief History of Signal

25 years ago, the technological optimists among us saw enormous potential in the emerging Internet as a liberatory tool. Remember that old CBC segment[3] which praised "a computer network called Internet" as "modulated anarchy?" And while there are still powerful ways to securely communicate, co-ordinate and spread ideas online, it's clear that State and corporate entities are gradually capturing more and more of the online space and using it to subject us to increasingly intense forms of surveillance and social control[4].

The Internet has always been an arms race. In 1991, cryptographer, civil libertarian and peace activist[5] Phil Zimmerman created Pretty Good Privacy[6] (PGP), an open-source application for file encryption and end-to-end encryption for email. I'm avoiding technical details, but basically the importance of end-to-end is that you can securely communicate directly with another person, and your email service can't see the message, whether it's Google or Riseup. To this day, as far as we know, PGP encryption has never been broken[7].

---

[3]https://www.youtube.com/watch?v=bl0wS1304jo

[4]Internet-era modes of governance vary from place to place—more authoritarian States might prefer filtering and censorship, while democratic States produce a kind of "digital citizenship"—but mass surveillance and cyber warfare are becoming the norm.

[5]Ironically, the U.S. Government would later attempt to charge Zimmerman with freely publishing PGP source code, arguing that he was "exporting weapons." So he published the source code in a hardcover book and mailed them around the world, the rationale being that the export of books is protected under the U.S. Constitution.

[6]https://openpgp.org

[7]Court cases against the Red Brigades in Italy (2003) and child pornographers in the U.S. (2006) have shown that federal police agencies failed to break into PGP-se-

For years, techies and security nerds in certain circles—anarchists, journalists, criminals, etc.—tried to spread PGP to their networks as a kind of secure communications infrastructure, with some success. As with everything, there were limitations. My biggest security concern with PGP is the lack of Forward Secrecy, which means that if a private encryption key is ever compromised, all the emails ever sent with that key can be decrypted by an attacker. This is a real concern, given that the NSA is almost certainly storing all your encrypted emails somewhere, and one day quantum computers might be able to break PGP. Don't ask me how quantum computers work—as far as I'm concerned, evil fucking magic.

The big social problem with PGP, one that strongly informed the Signal project, is the fact that it was never widely adopted outside of niche circles. In my experience, it was even difficult to get anarchists on PGP and using it properly. There were workshops, lots of people got set up, but as soon as a computer crashed or a password was lost, it was back to square one. It just didn't stick.

Sometime around 2010, smartphones started to popularize and everything changed. The ubiquity of social media, constant instant messaging, and the ability for telecom companies (and thus government) to track users' every move[8] has completely transformed the threat model. All the work people put into computer security was set back decades: smartphones rely on a completely different architecture than PCs, resulting in far less user control, and the advent of completely unfettered app permissions has made the idea of smartphone privacy almost laughable.

This is the context that Signal emerged from. Anarchist "cypherpunk" Moxie Marlinspike[9] started working on software to bring end-to-end encryption to smartphones, with Forward Secrecy, working on the idea that mass surveillance should be countered with mass encryption. Signal was designed to be usable, pretty, and secure. Moxie agreed to team up with

---

cured devices and communications. Instead, agents have resorted to bugging devices, passing legislation requiring you to surrender passwords, and of course, informants and undercover infiltration.

[8]Want to read something scary? Look up Google's Sensorvault.

[9]https://moxie.org

tech giants WhatsApp, Facebook, Google and Skype to implement Signal's encryption protocol onto their platforms as well.

> "The big win for us is when a billion people are using WhatsApp and they don't even know it's encrypted."
>
> — *Moxie Marlinspike*

Understandably, anarchists are more likely to trust their communications to Signal—a non-profit foundation run by an anarchist—than they are to trust big tech, whose main business model is harvesting and reselling user data. And Signal has some advantages over these other platforms: it's open-source (and thus subject to peer review), encrypts most metadata, stores as little user data as possible, and offers some very useful features like disappearing messages and safety number verification to guard against interceptions.

Signal has earned nearly universal praise from tech security experts, including endorsements from NSA whistleblower Edward Snowden[10] and top scores from the respected Electronic Frontier Foundation[11]. In 2014, leaked documents from the NSA described Signal as a "major threat" to its mission (of knowing everything about everyone). Personally, I trust the encryption.

But Signal only really protects one thing, and that's your communication as it travels between your device and another device. That's great, but it's only one piece of a security strategy. That's why it's important, when we talk about security, to start with Threat Modeling[12]. The first questions for any security strategy are who is your expected adversary, what are they trying to capture, and how are they likely to go about getting it. The basic idea is that things and practices are only secure or insecure relative to the kind of attack you are expecting to defend against. For example, you might have your data locked down with solid encryption and the best password, but if your attacker is willing to torture you until you give up the data, it doesn't really matter.

---

[10] https://web.archive.org/web/20220119200511/https://twitter.com/Snowden/status/661313394906161152

[11] https://eff.org

[12] https://en.wikipedia.org/wiki/Threat_model

For the purpose of this text, I would propose a working threat model that is primarily concerned with two types of adversaries. The first is global intelligence agencies or powerful hackers engaging in mass surveillance and intercepting communications. The second is police agencies, operating on territory controlled by the Canadian or American government, engaging in targeted surveillance of anarchists. For the police, basic investigative techniques include monitoring email lists and social media, sending undercovers to events, and casual informants. At times when they have more resources, or our networks become a bigger priority, they escalate to more advanced techniques including longer-term infiltration, frequent or continuous physical surveillance (including attempts to capture passwords), bugging devices, intercepting communications, and house raids where devices are seized and subjected to forensic analysis.

I should note that many European jurisdictions are implementing key disclosure laws[13] which legally compel individuals to give their passwords to authorities under certain conditions or face jail time[14]. Maybe it's only a matter of time, but for now in Canada and the U.S., we are not legally compelled to disclose passwords to authorities, with the notable exception of when we are crossing the border[15].

If your device is compromised with a keylogger or other malicious software, it doesn't really matter how secure your communications are. If you're hanging out with a snitch or a cop it doesn't really matter if you take the battery out of your phone and talk in a park. Device security and security culture are two concepts not covered by this text that have to be considered to guard against these very real threats. I've included a few suggestions in the “Further Reading”, p. 15 section.

It's also worth mentioning that Signal is not designed for anonymity. Your Signal account is registered with a phone number, so unless you register using a cash-bought burner phone or an online throwaway number, you're not anonymous. If you lose control of the phone number used to register

[13] https://en.wikipedia.org/wiki/Key_disclosure_law

[14] Plausible deniability, forward secrecy and secure data destruction are designed into some privacy tools to try and counter this threat or at least minimize its damage.

[15] Fingerprints (and other biometric data) are not considered passwords in many jurisdictions, meaning fingerprint locks are not subject to the same legal protections.

your account, someone else could hijack your account. That's why it's extra important, if you use an anonymous number to register your account, that you enable the "registration lock" feature.

Primarily for security reasons, Signal has become the standard communication medium in anarchist circles over the last 4 years, eclipsing everything else. But just as "the medium is the message," Signal is having profound effects on how anarchists relate and organize together that are too often overlooked.

The Sociality of Signal

> "Signal is useful to the extent that it replaces less secure forms of electronic communication, but it becomes harmful […] when it replaces face-to-face communication."
>
> — *Contributor*

Most of the social implications of Signal are not specifically about the app. They are the implications of increasingly moving our communications, personal expression, organizing efforts, and everything else onto virtual platforms and mediating them with screens. But something that dawned on me as I started sifting through questionnaire responses is that before Signal, I knew several people who outright rejected smartphones for both security and social reasons. When Signal emerged with answers to most of the security concerns, the holdout position was significantly eroded. Today, most of the holdouts have smartphones, either because they were convinced to use Signal or it became effectively mandatory if they wanted

to stay involved. Signal acted as a point of entry for some anarchists to smartphones.

On the other hand, insofar as Signal is harm reduction for those of us already ensnared by smartphones, that's a good thing. I'm glad that people who were primarily socializing and doing political organizing on unencrypted channels like Facebook switched to Signal. In my life, the group chat has replaced the "small email list" and is fairly useful for making plans with friends or sharing links. In the responses I collected, the Signal groups that were the most valuable to folks, or maybe just the least annoying, were the ones that were small, focused and pragmatic. Signal can also be a powerful tool for putting the word out quickly and securely about a pressing matter that requires a rapid response. If Facebook-based organizing has led too many anarchists to believe that organizing with any element of surprise is impossible, Signal has partially salvaged that idea, and I'm grateful for that.

Signal Fails

I first imagined this project as a short series of comic vignettes that I planned to call "Signal Fails," loosely modeled on the book "Come Hell or High Water: A Handbook on Collective Process Gone Awry[16]". Turns out it's hard to draw interesting pictures representing Signal threads and I suck at drawing. Sorry if I promised anyone that, maybe in the second edition… Either way, I still want to include some Signal Fails, as a way of making fun of us (I include myself in this!) and maybe to gently prod everyone to stop being so fucking annoying.

Bond, James Bond. Having Signal doesn't make you bulletproof. Give some people a little encryption, and they'll immediately subject their entire contact list to the absolute sketchiest shit. Your phone is still a tracking device, and trust is still built. Talk with your people about what kinds of things you feel comfortable talking about on the phone, and what you don't.

[16]https://web.archive.org/web/20240308061230/https://www.akpress.org/comehellorhighwater.html

Silence is not consent. Ever go to a meeting, make a plans with others, establish a Signal group to coordinate logistics, and then have one or two people rapidly change your collective plans by a rapid series of texts that no one has time to respond to? Not cool.

Hell is an endless meeting. A Signal group isn't an ongoing meeting. I'm already way too glued to my phone, so I don't like it when a thread is blowing up my phone and it's just a long side conversation between two people or someone's stream of consciousness that is unrelated to the purpose of the group. I appreciate it when conversations have beginnings and ends.

It wants to feed. I especially hate this one. Probably because of social media, some of us are used to information being curated for us by a platform. But Signal is not social media, thank fuck. So watch out because when a big Signal group starts becoming THE FEED, you're in trouble. That means if you're not on it and paying attention, you will miss out on all kinds of important information, whether it's upcoming events, people changing their pronouns, or flamewars that lead to social conflict. People start to forget you exist, and eventually, you literally disappear. Kill THE FEED.

Fire in a crowded theatre. Aka the panic button problem. You're chillin in a big Signal group with all your sketchy friends and all their actual phone numbers, someone gets pinched for shoplifting or something, and *surprise* their phone isn't encrypted! Everyone freaks and jumps ship, but it's too little too late, because if the cops are going through that phone right now, they can see everyone who left and the social mapping is done. Womp womp.

Mission creep. Someone created a Signal group to co-ordinate a specific, time-limited event. It's over, but no one wants to let go. Somehow, this very specific ad-hoc formation is now THE PERMANENT ORGANIZATION that has tasked itself with deciding everything to do about all things—indefinitely.

Towards Shared Practices

If you thought this was a guide to best practices on Signal or chat etiquette, I'm sorry you made it this far without realizing it's not. This is way more of a "we need to talk about Signal" kind of thing. I do believe in developing shared practices within specific social contexts, and recommend we start having this conversation explicitly in our networks. To that end, I do have a few proposals.

There are some obstacles to shared practices. Some people don't have Signal. If that's because they're building relations without smartphones, I have only respect for that. If it's because they spend all day on Facebook but Signal is "too hard," I don't buy it. If nothing else, Signal is easy to install and use for anyone with a smartphone and an Internet connection.

I also disagree with the Orwellian-fatalist perspective that sees encryption as pointless: "The cops know everything already!" It's super disempowering to understand government this way, and thankfully it's not true —resistance is not yet futile. CSEC or the NSA do have nightmarish capabilities, including many that we don't know about yet. But there is also ample evidence that encryption is frustrating police investigations, which is why governments are passing laws to thwart these tools.

Perhaps the biggest obstacle to shared practices is a general lack of a "we"—to what extent are we accountable to anyone, and if so to whom? How do we go about ethically constructing shared social norms? Most anarchists agree that it's wrong to snitch, for example, but how did we get there? I do think that a kind of vulgar liberal individualism is influencing

anarchism and making the very question of "expectations" almost taboo to discuss. But that's a different text for another day.

A Few Proposals for Better Practices

1. **Keep it IRL**. As one contributor put it, "Communication is not just about sharing information." Face to face communication builds whole relationships, including trust, and continues to be the most secure way to communicate.
2. **Leave your devices at home**. At least sometimes? Especially if you're going across the border, where you can be forced to decrypt your data. If you need a phone when you travel, purchase a travel phone with your friends that doesn't have any sensitive data, including your contact list, on it.
3. **Secure your devices**. Most devices (phones and computers) now have the option for full disk encryption. Encryption is only as good as your password and protects your data "at rest", i.e. when your device is OFF or the data is not being used by programs. Your lock screen provides some protection while your device is ON, but can be bypassed by a sophisticated attacker. Some operating systems force you to use the same password for encryption and your lock screen, which is unfortunate as it's not practical to enter a long password 25 times a day (sometimes in the presence of prying eyes or surveillance cameras).
4. **Turn off your devices**. If you leave your device unattended, or you're going to sleep, turn it off. Buy a cheap alarm clock. If your house is ever raided overnight you'll be glad you did. If your device is off and encrypted with a strong password when it's seized, cops are far less likely to be able to break into it. If you really want to go the extra mile, acquire a decent safe and lock your devices inside when you're not using them, which will reduce the risk of them being covertly physically tampered with.
5. **Establish boundaries**. We have different senses of what's safe to talk about on our phones and what's not. Discuss and develop col-

lective boundaries, and where we disagree, respect other people's boundaries even if you think it's safe.

6. **Agree on a vouching system**. If you're in a group discussing sensitive things, develop an explicit collective understanding of what constitutes a vouch for a new person to join. In an era where anarchists catch conspiracy charges, miscommunications about this can land people in jail.
7. **Ask first**. If you're going to add someone to a thread, thereby revealing their phone number to the entire group, ask for their and the group's consent first.
8. **Minimize decision-making**. Consider leaving decisions other than yes/no for in person meetings, if possible. In my experience, Signal impoverishes any decision-making process.
9. **Defined purpose**. Ideally, a Signal group will have a specific purpose. Each new person added to that group should have that purpose clearly explained to them. If that purpose has been served, leave the group and delete it.
10. **Disappearing Messages**. Very useful for housekeeping. Ranging from 5 seconds to 1 week, Disappearing Messages can be set by selecting the stopwatch icon in the top bar of a conversation. Many people use a standard 1-week disappearing time on all messages, whether the conversation is sensitive or not. Select your expiration time based on your threat model. This also protects you somewhat if the person you are communicating with is using less-than-ideal phone security practices.
11. **Verify safety numbers**. This is your best protection against a man-in-the-middle attack. It's quite simple to do and easiest in person —open your conversation with the person you want to verify with and navigate to "Conversation Settings > View safety number" and scan the QR code or compare numbers. Most respondents said "I should do this, but I don't." Take advantage of big gatherings to verify contacts. It's OK to be a nerd!
12. **Enable the Registration Lock**. Enable this in Signal's Privacy Settings, so if someone is ever able to hack your phone number used to register your account, they still have to get your PIN to hi-

jack your identity. This is especially important for anonymous Signal accounts registered with burner numbers, since someone else will almost certainly use this number again.

13. **Turn off message previews**. Keep messages from appearing on your lock screen. On my device, I had to set this on my device settings (not Signal settings) under "Lock Screen Preferences > Hide Sensitive Content".
14. **Delete old messages**. Either by enabling thread trimming or manually deleting completed conversations, don't keep messages around that you don't need anymore.

Conclusion

I embarked on this project to reflect and gather feedback on the impact Signal has had on anarchist networks in the U.S. and Canada, from the standpoint of both security and social organization. In doing so, I think I hit on some common frustrations people have, especially with large Signal groups, and gathered together a few proposals to circulate. I continue to insist that smartphones are doing more damage than good to our lives and struggles, because it's important to me. We need to preserve and build other ways of organizing ourselves, especially offline, for both quality-of-life and movement security. Even if we stick with smartphones, it's dangerous when our communications are centralized. If Signal's servers went down tonight, or Riseup[17], or Protonmail[18], imagine how devastating that would be to our networks. If anarchists ever pose a major threat to the established order, they will come for us and our infrastructure without mercy, including suspending "legal protections" we might be depending on. For better and for worse, I believe this scenario to be possible in our lifetime, and so we should plan for resilience.

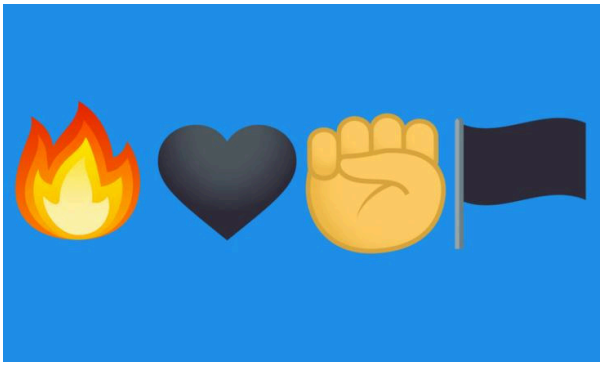
The techies among us should continue to experiment with other protocols, software and operating systems[19], sharing them if they prove useful.

[17] https://riseup.net

[18] https://protonmail.com

[19] On my phone, I recently replaced Android with LineageOS, which is a privacy-oriented, de-Googled operating system based on Android code. It's great, but it's only

The holdouts should keep holding out, and find ways to thrive offline. For the rest of us, let's minimize the degree to which we're captured by smartphones. Along with a capacity to struggle, we should build lives worth living, with a quality of relationships that potential friends and co-conspirators find irresistibly compelling. It might be the only hope we've got.



Further Reading

This zine was published in May 2019. Signal periodically updates its features. For the most up-to-date information about technical stuff, go to signal.org, community.signalusers.org, and /r/signal[20] on Reddit.

- Your Phone is a Cop[21].
- Choosing the Proper Tool for the Task[22].
- EFF Tool Guides for Surveillance Self-Defense (including Signal)[23].
- Towards a Collective Security Culture[24].
- Riseup Security Guide[25].
- Toronto G20 Main Conspiracy Group: The Charges And How They Came To Be[26].

---

built for certain devices, you void your phone warranty, and there's definitely a learning curve when it comes to setting it up, keeping it updated and switching to open-source software.

[20]https://reddit.com/r/signal

[21]https://itsgoingdown.org/phone-cop-opsecinfosec-primer-dystopian-present

[22]https://crimethinc.com/2017/03/21/choosing-the-proper-tool-for-the-task-assessing-your-encryption-options

[23]https://ssd.eff.org/en/module-categories/tool-guides
[24]https://crimethinc.com/2009/06/25/towards-a-collective-security-culture
[25]https://riseup.net/security
[26]https://notrace.how/resources/#toronto-g20-main-conspiracy-group

Signal is an encrypted messaging service that has been around in different forms for about 10 years. Since then, I have seen the software widely adopted by anarchist networks across Canada and the United States. More and more, for better and for worse, our interpersonal and group conversations have moved onto the Signal platform, to the extent that it has become the dominant way anarchists communicate with each other on this continent, with very little public debate about the implications.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.