# The Guide to Peer-to-Peer, Encryption, and Tor

## New Communication Infrastructure for Anarchists

Anonymous

2022-10-06

# Shhh...

This is a discussion about digital tools for communicating securely and privately. To begin, it must be stressed that a face-to-face meeting, out of sight of cameras and out of earshot from other people and devices, is the most secure way to communicate. Anarchists were going for walks to chat long before encrypted texting existed, and they should still do so now, whenever possible.

That being said, it's undeniable that secure digital communication tools are now part of our anarchist infrastructure. Perhaps many of us rely on them more than we should, but there is an extent to which they have become unavoidable for coordinating, collaborating, and staying connected. Given that these tools are essential infrastructure for us, it's crucial that we constantly scrutinize and re-evaluate their security and effectiveness at protecting our communications from our adversaries.

In the last decade or two, anarchists have been early adopters of these secure communication tools and techniques, and have played a role in normalizing and spreading their use within our own communities, as well as among others engaged in resistance and struggle. The following text is intended to present anarchists with newer tools for secure encrypted communication, and make the case that we should adopt them in order to bolster the resilience and autonomy of our infrastructure. We can learn the advantages of these new apps – how they can help dodge surveillance and repression – and subsequently employ them effectively in our movements and help spread their use more broadly.

It is easiest to frame a conversation about new secure chat apps by presenting them in contrast to the secure chat app everybody knows: Signal. Signal is the *de facto* secure communication infrastructure for many, at least in North America, and it is rapidly becoming ubiquitous outside of anarchist circles. If you are reading this you probably use Signal, and there is a good chance your mom or co-worker uses Signal too. Signal's usage surged massively in January 2021 (so much so that the service was knocked out for 24 hours), reaching 40 million daily users. Signal allows users to very easily exchange encrypted messages. It grew out of an earlier project called TextSecure, which added encryption to SMS messages (old fashioned text-messages for the zoomers reading). TextSecure, and later Signal, were both rightfully trusted by anarchists early on, in large part because of the IRL web-of-trust between the core developer, Moxie Marlinspike, and other anarchists.

At the beginning of 2022 Moxie left Signal, and this spurred a new wave of conspiracy-tinged fearmongering. *The anarchist CEO of Signal has resigned. Signal is cancelled*. A piece titled "Signal Warning" published on *It's Going Down*[1] attempted to dispel these worries and conspiracy theories, and discussed whether anarchists can still 'trust' Signal (they can, with caveats as always), and reiterated why Signal is, actually, quite secure and trustworthy (it is heavily audited and examined by

security experts).

However, "Signal Warning" did suggest Moxie's departure marked, at the very least, a reminder of the necessity of constant scrutiny and skepticism of Signal, and of any third party tool or software anarchists use.

> Now, with the veneer lifted, our ability to analyze Signal, and to evaluate its usage within our contexts can begin to occur outside of any distortions that trust can sometimes generate. Now we have to look at the app and its underlying protocol as they are, as code running within a computer, with all of the benefits and limitations that this entails. This is far from the end, and is not even, at this point, even moving in that direction. But, like all technical systems we need to approach them with information and suspicion.

Signal continues to be widely trusted, and there is still nothing close to a "smoking gun" regarding Signal's security. What follows is not a call to abandon Signal – Signal remains an excellent tool. But, given its outsized role in anarchist infrastructure and renewed interest in whether we can or should trust Signal, we can take this opportunity to closely examine the app, how it works, how we use it, and explore alternatives.

Close scrutiny of Signal does not reveal secret backdoors, or gaping vulnerabilities. But it does reveal a prioritization of user experience and streamlined development over the most robust security goals. The broader project goals and features of Signal now may not exactly fit our threat model. And because of how Signal works at a structural level, anarchists are reliant on a centralized service for the bulk of our secure online communications. This has consequences for security, privacy, and reliability.

But there are alternatives that have been developed in large part to specifically address these issues. Briar and Cwtch are two newer secure chat applications that, like Signal, also allow the exchange of encrypted messages. On the surface, they seem to function very much like Signal, but how they actually work is quite different. Where Signal is an encrypted messaging service, by contrast Briar and Cwtch are **PET** apps – they are self-contained applications that permit **P**eer-to-peer and **E**ncrypted messaging over **T**or.

These PET apps and how they work will be presented in detail. But the best way to really explain their advantages (and why anarchists should even care about other secure chat apps when we already have Signal) is to undertake a deep-dive critical analysis of Signal.

[1] https://itsgoingdown.org/signal-warning-why-moxies-departure-is-not-the-end-of-signal/

# Threat Model and Disclaimers

Before diving in, it's important to contextualize this discussion by defining the relevant threat model and to provide some disclaimers.

For the purposes of this discussion, our adversaries are Nation-State-level law enforcement, or local law enforcement with some access to Nation-State-level law enforcement resources.

Despite end-to-end encryption hiding the contents of messages in transit, these adversaries have many capabilities which could be used to uncover or disrupt our activities, communications, or networks so they can repress us. In particular, the following capabilities of these adversaries will be addressed:

- They have trivial access to social media sites and other public information.
- In some cases, they can monitor all home or cell phone internet traffic for a specific targeted individual.
- They can access "anonymized" user data or metadata from apps, cell phone providers, ISPs, etc.
- They can access recorded network traffic collected en-masse from many bottlenecks in internet infrastructure.
- To varying degrees of success they can combine, analyze, and correlate such data and network traffic in order to de-anonymize users, map social networks, or reveal other potentially sensitive information about individuals or groups and their communications.
- They can compromise internet infrastructure (isps, service providers, corporations, app developers) either though coercion or hacking.[2]
- They can disrupt internet traffic in general or in targeted ways, either because they control internet infrastructure, or by wielding cyberattacks against internet infrastructure.

This guide is concerned with mitigating against the above capabilities of these adversaries, but there are many others that cannot be addressed here:

- They can remotely infect devices of targeted individuals with keylogger and tracking malware, in extreme cases.
- They can gain access to encrypted communication via confidential informants or undercover agents.
- They can wield great pressure or torture to compel individuals to unlock their phone or computer or give up passwords.
- Although they cannot break good encryption within any practical timeframe, in the case of a seizure they may still be able to obtain data from ostensibly

[2] By hook or by crook.

encrypted devices due to other vulnerabilities (e.g. in the device's operating system) or operational security failures.

Any secure communications method is highly dependent on the surrounding security practices of the user. It doesn't matter if you are using *Edward Snowden's Preferred Secure Chat App™* if your adversary has a keylogger installed on your phone, or if someone shares screenshots of your encrypted texts on Twitter, or if your phone is seized and not properly secured.[3]

A full explanation of operational security, security culture, and related concepts and best practices is outside the scop of this text – this discussion is only *one part* of the operational security relevant to the working threat model. You must consider general security culture to protect against the threat of infiltrators and informants, how to safely use devices like phones and laptops so they can't help to build a case if seized, and how to build habits to minimize the data left on electronics devices entirely (meet face-to-face and leave your phone at home!).

So-called "cybersecurity" is fast-moving: there is a war of attrition between threats and app developers. Information provided here may be out of date by the time you are reading this. Application features or implementations may change, partially invalidating some of the arguments made here (or bolstering them). If the security of your electronics communications is crucial to your safety, you should not trust *any* recommendation given here or elsewhere at face value.

# Signal Loss

You probably used Signal today. And nothing is really *that* wrong with Signal. It is important to state that despite the following critiques, the goal here is not to incite a panic about using Signal. Your takeaway shouldn't be to immediately delete Signal, burn your phone, and run into the woods. Maybe you should do that anyways for your own mental health but like, not just because of this guide. Consider going on a hike first at least.

## A Tangent to Deal With Some Conspiracy Theories

A quick duckduckgoing (or maybe search on Twitter? I wouldn't know) for "Signal CIA" will bring up plenty of disinformation and conspiracy theories about Signal. Given the already critical nature of this guide and the importance of nuance, please permit a rant about these conspiracy theories.

The most common conspiracy theory about Signal is that it was secretly developed by the cia and therefore is "backdoored." Consequently, the CIA (or sometimes

[3] https://pugetsoundanarchists.org/snitches-sleuths-an-update-from-puget-sound-prisoner-support/

the NSA) has the ability to easily access everything you say on Signal by poking in through their secret back door.[4]

The spark of truth that ignited this theory is as follows:

> Between 2013 and 2016, Signal's developers received just under 3 million usd in funding from the Open Technology Fund. The otf was originally a program of Radio Free Asia which is supervised by the U.S. Agency for Global Media (since 2019, the otf is directly funded by the USAGM). The USAGM is an "independent agency of the U.S. government", that promotes U.S. national interests internationally and is funded and managed directly by the U.S. government. The U.S. government manages and funds usagm/Radio Free Asia, which funds the OTF, which funded Signal's development (and Hilary Clinton was Secretary of State at the time!!) – thus, the CIA created Signal.

The USAGM (and all its projects like Radio Free Asia and the OTF) promotes U.S. national interests by undermining or disrupting governments the U.S. is in competition or conflict with. Besides promoting contrary media narratives (via supporting a "free and independent press" in these countries) this also involves producing tools that can be used circumvent censorship and resist "oppressive regimes".

Beneficiaries of the OTF are transparently disclosed[5] and it is not a secret that the OTF's goal is to create tools to subvert the power of regimes that rely heavily on overt online repression, mass surveillance, and strong internet censorship to maintain their power (and that these regimes are ones the U.S. government happens to not be a fan of). How and why this happens in relation to projects like Signal is plainly reported by mainstream outlets like the Wall Street Journal.[6] Outlets like RT also report this same information without context and with sensational embellishment[7] leading to these conspiracy theories.

Signal is open-source, which means all of its code is audited and scrutinized by experts. It is the one place everyone is looking for a CIA backdoor. In terms of mass surveillance, it is easier and more effective for our adversaries to covertly insert surveillance into widely used closed-source internet applications and infrastructure with the cooperation of complicit corporations.[8] In terms of targeted surveillance, it is easier to install malware on your phone.[9]

Many open-source software projects like Signal have received funding from similar sources. The OTF also funds or has funded numerous other projects you may

[4] See the FBI honeypot encrypted chat app Anom for a real-life example of this https://www.vice.com/en/article/akgkwj/operation-trojan-shield-anom-fbi-secret-phone-network

[5] https://www.opentech.fund/results/supported-projects/open-whisper-systems/

[6] http://www.wsj.com/articles/moxie-marlinspike-the-coder-who-encrypted-your-texts-1436486274

[7] https://www.rt.com/op-ed/513732-signal-messenger-us-national-security/

[8] https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

[9] https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092

have heard of: Tor (about which similar conspiracy theories exist), K-9 Mail, NoScript, F-Droid, Certbot, and Tails (whose developers include anarchists).

This funding is always transparently disclosed. Just check the sponsors page of Tails[10] where you can see OTF listed as a past sponsor (and that their current top sponsor is… the U.S. State Department!). Both of the PET apps discussed in this guide are partly funded by similar sources.

There is an endless discussion to be had about funding sources of open-source projects that facilitate privacy or surveillance-resistance: conflicts of interest, ethics, trustworthiness, such tools being developed in the context of neoliberal geopolitics… It is good to have a healthy skepticism and critique about how projects are funded, but it should not lead us to conspiracy theories that cloud discussions about their actual security in practice. Signal has received funding from many such "dubious" sources: Signal's initial development was funded by the sale of its precursor project, TextSecure, to Twitter for an unknown amount. More recently Signal was given a $50 million USD, 0% interest loan from the founder of WhatsApp, who is now the ceo of the Signal Foundation. There is plenty of valid evidence explaining why and how Signal was funded by some initiative of the US's drive for global dominance that does not in any way suggest or imply the existence of some impossible-to-hide cia backdoor meant to target Signal users.

## Signal is Fine Actually?

So if Signal is not a CIA op, then it's all good right? Signal's encryption protocols are widely regarded as secure, and Signal has a great track record of improving its features and addressing vulnerabilities in a timely and transparent manner. Signal managed to successfully make end-to-end encrypted chat easy enough to actually become popular. Widespread adoption of Signal is almost certainly a good thing.

But conspiracy theories aside, there are good reasons for anarchists to be skeptical of Signal. Moxie had a somewhat dogmatic approach to many software engineering and structural choices made in Signal's development. These decisions were made intentionally (as explained in blog posts, talks, and in various arcane GitHub issue threads) to facilitate the widespread adoption of Signal Messenger among less tech-savvy users, ease long-term growth of the project, and allow streamlined evolution and the addition of new features.

Online cybersecurity gadflies have long critiqued these decisions as trade-offs that sacrifice better user security, privacy, or anonymity in the interest of Moxie's own goals for Signal. Getting too deep on this runs the risk of veering into the territory of debate dominated by pedantic fedora-clad FOSSbros (if we aren't there already). To keep it extremely brief, Moxie's justifications can be boiled down to keeping Signal competitive in the capitalist, profit-driven Silicon Valley ecosystem.

[10] https://tails.boum.org/sponsors/index.en.html

Debates about software development strategies under late capitalism aside, the nuts-and-bolts aspects of Signal most commonly critiqued are as follows:

1. Signal relies on a centralized server infrastructure
2. Signal requires every account to be linked to a phone number
3. Signal has a built-in cryptocurrency payment system

Maybe Moxie was right and his trade-offs were worth it: today, Signal is wildly popular, the app has scaled massively with minimal growing pains, numerous new features (both for usability and security) have been easily introduced, and it seems to be sustainable for the foreseeable future.[11]

But Signal's ubiquity as anarchist infrastructure demands careful examination of these critiques, especially as they apply to our use cases and threat model in a changing world. Examining these critiques of Signal will help explain how PET apps like Briar and Cwtch, which use a completely different approach to secure communication, can potentially provide us with more resilience and security.

## Signal as a Centralized Service

Signal is really less of an application and more of a service. Signal (Open Whisper Systems/The Signal Foundation) provides the Signal Application (which you can download and run on your phone or computer) and operates the Signal Server3. The Signal Application on its own cannot do anything. The Signal Server[12] provides the underlying service by handling and relaying all the messages sent and received with Signal.

This is how most chat apps work. Discord, WhatsApp, iMessage, Instagram/Facebook Messenger and Twitter dms are all centralized communication services, where you run an app on your device and a centralized server operated by some third party relays messages between individuals. Centralization like this provides many benefits to you as a user. You can sync your messages and profile over the server to access them on different devices. You can send a message to your friend even when they are offline and the server will store the message until your friend logs on and retrieves it. Group chats between many users work flawlessly even though users may be on- or offline at different times.

Signal uses end-to-end encryption, which means that the Signal Server cannot read any of your messages. But being a centralized communication service has many important implications for security and reliability.

[11] Although Signal does seem to really want more donations from users, despite sitting pretty on a $50 million USD loan.¯_(☒)_/¯

[12] Rather than a single physical server, this is actually a huge cloud network of servers rented in Amazon datacenters all over the U.S. – this can be abstracted to a single Signal server for the purposes of our discussion.

## The Signal Post Office

Consider how Signal-as-a-service is like a postal service. It's a really good postal service, like maybe they have somewhere in Europe. In this example, the Signal Server is like a post office. You write a letter to your friend and seal it in an addressed envelope (let's just say no one but your friend can open the envelope – that's the encryption). At your convenience, you drop off all the letters you are sending at the Signal Post Office, where they get sorted and sent out to the various friends they're addressed to. If a friend isn't home, no problem! The Signal Post Office will hold on to the letter until they catch your friend at home, or your friend can just pick it up at their local Signal Post Office. The Signal Post Office is really good (Europe, right?) and even lets you forward your mail anywhere you might want to receive it.

Maybe you can spot the potential security issue with relying on the Signal Post Office to handle all your mail. Sealed envelopes means that none of the mail carriers or employees at the Signal Post Office can read any of your letters (encryption = they can't open the envelopes). But anyone who has a regular mail carrier knows they can still learn a lot about you just by handling all your mail. They know who you are receiving letters from, all your magazine subscriptions, when you are home or not home, all the different places you forward your mail to, and all the embarrassing shit you order online. This is the potential problem with a centralized service handling all of your mail – I mean messages!

## Metadata is Forever

The information everyone at the Signal Post Office knows about you and your mail is *metadata*. Metadata is data *about* data. This can include things like the sender and recipient of a message, the time it was sent and where it was delivered. All traffic on the internet inherently generates this kind of metadata. Centralized servers provide an easy point where all that metadata could be observed or collected, since all messages pass through a single point.

It must be stressed that the above example about the Signal Post Office is just metaphorical to illustrate what metadata is and why it is a relevant concern for centralized communication services. Signal is actually *extremely good* at minimizing or obscuring metadata. Thanks to cryptographic black magic and clever software design, there is very little metadata that the Signal Server can easily access. In Signal's own words:

> Things we don't have stored include anything about a user's contacts (such as the contacts themselves, a hash of the contacts, any other derivative contact information), anything about a user's groups (such

> as how many groups a user is in, which groups a user is in, the membership lists of a user's groups), or any records of who a user has been communicating with.[13]

There are only two pieces of metadata which are known to be persistently stored:

- whether a particular phone number is registered to a Signal account
- the last time a given Signal account was connected to the server

This is good! In theory, that's all that any nosy employee at the Signal Post Office can know about you. But this is due, in part, to the "I do not see it" approach of the Signal Server itself. To a certain extent, we must trust the Signal Server is doing what it claims…

## No Choice but to Trust

Like the Signal application on your phone or computer, Signal's Server is also based on (mostly[14]) open-source code and therefore it is subjected to the same scrutiny and audits by security experts.

However, there is an important and unavoidable reality to consider about the Signal Server: we are forced to trust that the Signal Server is actually running the same open-source code that is shared with us. This is a fundamental problem with relying on any centralized server run by a third party.

> "We do not collect or store any sensitive information about our users, and that won't ever change."[15]

As a huge public non-profit, Signal is not in a position to sustainably refuse to comply with warrants or subpoenas for user data. Signal even has a page on their website[16] which lists several subpoenas they have received and their responses. Recall the two pieces of metadata the Signal Server does store that can be disclosed:

At the time of writing there is no reason to doubt what has been disclosed, but it should be noted that Signal also complies with gag orders preventing them

[13] https://signal.org/bigbrother/eastern-virginia-grand-jury/

[14] Recently, Signal opted to make some of their server code closed-source, ostensibly to allow them to combat spam on the platform (see https://signal.org/blog/keeping-spam-off-signal/). This means there is now a small piece of the Signal Server code that is not shared publicly. This change also denotes an increase, albeit extremely minimal, in server-side metadata collection since it is necessary to facilitate effectively fighting spam even in a basic way. There is no reason to suspect foul play here, but it is important to note that this is yet another policy decision that sacrifices security concerns in the interest of user experience.

[15] https://signal.org/blog/sealed-sender/

[16] https://signal.org/bigbrother/

| Account | Responsive Information in Signal's Possession |
|---|---|
| [redacted] | Last connection date: 1634169600000 (unix millis)<br>Account created: 1606866784432 (unix millis) |

Signal's responses show last connection date, account creation date, and phone number (redacted).

from disclosing that they have even received a subpoena or warrant.[17] Historically, Signal fights these gag orders, but we don't know what we don't know, and Signal does not employ a 'warrant canary' to alert users of any subpoenas or warrants that have not yet been disclosed. There is no firm reason to believe that Signal has cooperated with law enforcement either more frequently or to a greater extent than they claim, but there are three scenarios to consider:

1. Changes in the law could result in Signal being compelled to collect and disclose more information about its users on request, and this could happen without public knowledge.
2. Signal could be convinced by ethical, moral, political, or patriotic arguments to secretly cooperate with adversaries.
3. Signal could be infiltrated or hacked by adversaries to collect more user data in secret, or otherwise provide what little metadata there is more readily to adversaries.

These scenarios are all conceivable and have historical precedents elsewhere, but they are not necessarily probable or likely. Due to the aforementioned "cryptographic black magic" and the complexities of network protocols, even if Signal Server was modified to be malicious, there is still a limit to how much metadata could be collected without it being noticed by users or observers. It would *not* be equivalent to, say, the Signal Post Office letting in a spy (through a literal "CIA backdoor!") who reads and records all the metadata for every letter passing through. Changes in Signal's policies and code *could* result in small but increasing amounts of metadata, or other information, being readily available to adversaries, and this could happen with or without our knowledge. There is no particular reason to *distrust* the Signal Server at this point, but anarchists must weigh how much trust they are placing in a third party, even one as historically trustworthy as Signal.

[17] https://signal.org/blog/looking-back-as-the-world-moves-forward/

## Big Data

Many powerful adversaries are capable of capturing and storing massive amounts of traffic on the internet.[18] This can include actual message contents for unencrypted traffic, but with widespread use of encryption, it is now mostly metadata about everyone's internet traffic and activity that is captured and stored.

We can choose to trust that Signal is not actively assisting our adversaries in collecting metadata about Signal users' communications, but our adversaries have many other ways to collect this data: either with the cooperation of hosting companies like Amazon or Google (Signal is currently hosted by Amazon Web Services), by targeting such hosting companies without their cooperation,[19] or by simply monitoring internet traffic at a mass scale.[20]

Metadata about everyone's activities online is also increasingly available to less-powerful adversaries, who are able to purchase it in raw or analyzed form from data brokers, who in turn purchase or acquire it from entities like app developers or cell phone providers.[21]

Metadata collected in this way results in large, unwieldy data sets which were previously difficult to analyze. But increasingly our adversaries (and even corporations or journalists) can take these huge data sets, combine them, and apply powerful algorithmic analysis tools to yield useful correlations about individuals or groups of people (this is often referred to as "Big Data"). Even access to small amounts of this data and crude analysis techniques can de-anonymize individuals and yield useful results.[22]

## Tommy Texter

This is a hypothetical example to demonstrate how traffic analysis and correlation of metadata can de-anonymize a Signal user.

Imagine a frequent, but badly behaved movie-goer named Tommy who is always texting on Signal during the movie. The glare of his phone screen (Tommy doesn't use dark mode) annoys everyone in the theatre. But it's otherwise too dark in the theatre for Tanner, the busybody manager, to figure out exactly who is always texting. Tanner starts collecting all the data passing through the theatre's Wi-Fi looking for connections to the Signal Server. Tommy's frequent connections

[18] https://www.nationalgeographic.com/pages/article/130612-nsa-utah-data-center-storage-zettabyte-snowden

[19] https://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/

[20] https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/

[21] https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data

[22] For an example, see this story about Catholic investigative journalists who busted a priest for using Grindr by purchasing app data and denonymizing it to identify him: https://www.pillarcatholic.com/p/pillar-investigates-usccb-gen-sec

to the Signal Server stand out right away. Tanner is able to record the MAC address (a unique identifier associated with every phone) and confirm that the same device is frequently using Signal on the theatre's Wi-Fi during showtime. Tanner is then able to correlate this with credit card transaction records from their box office and discover a credit card that always buys tickets to movies around the same time the frequent Signal-using device is active (the card holder's name is also revealed: Tommy). Having determined Tommy's phone's MAC address, name, and credit card, Tanner can provide this information to a shady private investigator, who will purchase access to large datasets collected by data brokers (from cell phone providers and mobile apps), and determine a location where the same cell phone is most frequently used. Besides the movie theatre, this is Tommy's home. Tanner goes to Tommy's home at night and fire-bombs his car (the movie theatre is a front for the Hell's Angels).

## Weaponized Metadata

> "We kill people based on metadata... ...but that's not what we do with this metadata!" (knowingly smiles, laughter erupts from audience)[23]
>
> – General Michael Hayden, former NSA director 1999-2005 and CIA director 2006-2009

On an internet where adversaries have these capabilities to collect and analyze huge amounts of metadata and traffic, using centralized servers can be a liability. Adversaries can more easily target devices talking to the Signal Server either by monitoring traffic on the internet in general, at the ISP level, or potentially at connection points to the Signal Server itself. They can then *try* to employ analysis techniques to reveal specific things about individual users or their communications over Signal.

In practice this *can* be difficult. You may wonder if an adversary observing all the traffic going in and out of the Signal Server could determine that you and your friend exchange messages by noting that a message was sent from your IP address to the Signal Server at 14:01 and then the Signal Server sent a message of the same size to your friend's IP address at 14:02. Thankfully, very simple correlational analysis like this is not possible both because of the amount of traffic flying in and out of the Signal Server all the time and how exactly that traffic is handled at this level. This is less true for video/voice calls where the internet protocols in use make correlational traffic analysis to figure out who called who more plausible.[24] Still, an adversary observing all the traffic going in and out of the Signal Server and trying to determine

[23] https://www.youtube.com/watch?v=kV2HDM86XgI (quote is at the 18 min mark)

who is talking to who has a very difficult task. Maybe impossible, so far.

And yet, the data gathering techniques, and algorithmic analysis tools commonly referred to as "Big Data" are becoming more powerful every day. Our adversaries are at the cutting edge of this. Widespread use of encryption of all telecommunications has made traditional eavesdropping much less effective and consequently our adversaries are strongly motivated to increase their ability to gather and usefully analyze metadata. They say it plainly: *"if you have enough metadata, you don't really need content."*[25] They kill people based on metadata.

So although it may not be possible to determine with certainty something as precise as who talked to who at a specific time, our adversaries are still rapidly improving their ability to determine whatever sensitive information they can from metadata. They are routinely revealed through leaks to have been in possession of more powerful or invasive surveillance capabilities than previously thought – it is not unreasonable to project that their capabilities are more advanced than we know.

Signal is more vulnerable to this kind of surveillance and analysis because it is a centralized service. Signal traffic on the internet is not difficult to spot, and the Signal Server provides an easy central point to observe or collect metadata about Signal users and their activities. Potential compromises of Signal, or changes in their policies or the law could yield even easier collection of Signal traffic and metadata for our adversaries to analyze.

Individual users can employ some mitigations against this, such as running Signal through Tor or a VPN, but this can be technically challenging to implement and prone to user error. Any effort to make it harder to link a Signal user to a specific individual is also complicated by the fact that Signal requires every account to be linked to a phone number (more on that later).

## Dependency and Single Points of Failure

A centralized service means not only is there a central observation point, but there is also a single point of failure – Signal doesn't work if the Signal Server is down. It's easy to forget this is the case until the day when it happens. Signal can make a configuration mistake or get hit with a flood of new users because of a viral Tweet and all of a sudden Signal just doesn't work.

Signal could also go down because of intentional actions taken by an adversary. Imagine a Distributed Denial of Service attack (or other cyberattack) meant to disrupt Signal's function during a mass rebellion. The service providers that actually host the Signal Server could also choose to take down the Signal Server without

[24] See an example, which has since been patched, here: https://medium.com/tenable-techblog/turning-signal-app-into-a-coarse-tracking-device-643eb4298447

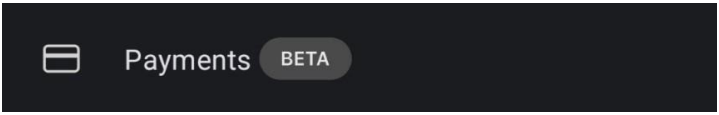
[25] NSA General Counsel Stewart Baker.


warning for a variety of reasons: compelled by pressure from an adversary, by political pressure, by public opinion, or for financial reasons.

A centralized service is also easier to disrupt by adversaries who directly control their local internet infrastructure.[26] When this happens in certain places, Signal is usually quick to respond by actively implementing creative changes or workarounds, resulting in a cat-and-mouse game between Signal and whatever Nation-State is attempting to block Signal within their area of control. Again, it is a matter of trusting that Signal's interests will always align with our own when an adversary is attempting to disrupt Signal in this way in a particular region.

## Cryptocontroversy

In 2021, Signal started to integrate a payment system into the app using the cryptocurrency MobileCoin. If you had no idea, you are probably not alone, but it's right there on your Settings screen.




MobileCoin is a little-known, privacy-focused cryptocurrency that Moxie also helped develop. Debates about cryptocurrency pyramid schemes aside, the concern here is that by including cryptocurrency payments inside the app, Signal is opening itself to much greater legal scrutiny from law enforcement. Cryptocurrencies are good for crime and scams, and the U.S. government is increasingly concerned with regulating their use. Signal is not a band of pirates – they are a high-profile nonprofit, and they cannot sustainably resist whatever new laws the U.S. government may pass to regulate cryptocurrencies.

[26] OONI report on current apparent blocking of Signal: https://explorer.ooni.org/search?until=2021-07-13&since=2021-06-12&test_name=signal&failure=false&only=anomalies

If Signal's millions of users were indeed using MobileCoin for daily transactions, it is not difficult to imagine Signal facing greater scrutiny from the U.S.'s Securities and Exchange Commission, or other regulatory bodies. The government doesn't like encryption, but they *really* don't like regular people paying for drugs or avoiding taxes. Imagine a scenario where cybercriminals rely on Signal and MobileCoin to accept payments from ransomware victims. It could really bring the heat, and this could be very disruptive to Signal as a reliable and secure communication tool.

## 514-U-SNITCH

This frustration should already be familiar to anarchists using Signal: Signal accounts require a phone number. Whatever phone number an account is linked to is also disclosed to anyone you connect with on Signal. Furthermore, determining if a given phone number is linked to an active Signal account is trivial.

There are workarounds for this problem, but they all involve obtaining a phone number that isn't tied to your identity just so you can use it to register for a Signal account. Depending on where you are, the resources available to you, and your technical skill level, this can range from inconvenient to prohibitively difficult.

Signal also does not easily allow multiple accounts to be used from the same phone or laptop. Setting up multiple Signal accounts for different identities, or to associate with different projects, becomes a huge task, especially since you need a distinct phone number for each one.

It's usually fairly easy for adversaries with limited resources to identify an individual based on their phone number. Furthermore, if an adversary obtains a phone that is not properly shut down or encrypted, they gain access to the phone numbers of contacts and group members. Obviously this is an operational security issue that goes beyond Signal, but the fact that Signal requires every account to be linked to a phone number greatly compounds the potential for network mapping and damaging fallout.

Whether Signal will ever allow accounts to exist without being linked to a phone number, or some other similar real-life identifier, is not known. It's been reported as something they will never do, or something they are working on but is forever in limbo.[27] Either way it's a major problem for many anarchist use cases.

[27] Forgive this extended note about phone numbers. Although Signal has mentioned being open to moving away from requiring a phone number in GitHub issue threads, there has not been any kind of official announcement that it is a coming feature under heavy development. Supposedly, one of the issues with dropping phone numbers for registration is that it will break compatibility with older Signal accounts due to how things were implemented in TextSecure days. This is ironic, given that Moxie's main argument against decentralized models are that it makes "moving fast" too hard – there is too much overhead to implement new features. And yet Signal is stuck with a much-maligned issue because of legacy code around registering accounts with a central server.

Moxie has also explained that phone numbers are used as the base of your identity in Signal to facilitate pre- serving your 'social graph.' Rather than Signal having to maintain some kind of social network on

# Heavy PETting

Having discussed Signal at length, it is time to introduce some alternatives that address some of the issues with Signal: Briar and Cwtch.

Briar and Cwtch are, by design, extremely *metadata-resistant*, and they provide better potential for anonymity. They are also more resilient, lacking a central server or single point of failure. But these advantages do come with costs – greater security comes with some quirks in usability that you have to get used to.

Recall, both Cwtch and Briar are **PET** apps because the are:

1. **P**eer-to-peer
2. like Signal, messages are end-to-end **E**ncrypted
3. user's identities and activities are anonymized by sending all messages through **T**or

Because they share a basic architecture, they have many common features and considerations.

## Peer-to-Peer

Signal is a centralized communication service, which uses a server to relay and transmit every message you send to your friend. The issues with this model have been discussed at length! You're probably bored of hearing about it by now. The **P** in PET is for *peer-to-peer*. In a peer-to-peer model you exchange messages directly with your friend. There is no intermediary central server run by a third party. Every direct connection only relies on the broader infrastructure of the internet.

Remember the Signal Post Office? With a peer-to-peer model, you don't use a postal service to handle your mail. You deliver every letter directly to your friend yourself. You write it, seal it in an envelope (end-to-end encryption), toss it in your messenger bag and bike across town where you hand deliver it to your friend.

---

your behalf, all your contacts are identified by their phone number in your phone's address book, making it easy to maintain and preserve your contacts list as you move from other apps to Signal, or if you get a new phone, or whatever. For Moxie, it sounds like having to 'rediscover' your contacts periodically at any point is a horrible incon- venience. For anarchists, it should be considered an advantage to have to intentionally maintain our 'social graph' based on our affinity, desires, and trust. Who is in our 'social graph' should be something we are con- stantly reevaluating and reexamining for security rea- sons (do I still trust everyone who has my phone number from 10 years ago) and to encourage intentional social relationships (am I still friends with everyone who has by phone number from 10 years ago).

Final trivia about Signal's use of phone numbers: Signal spends more money on verifying phone numbers than they do on hosting costs for the rest of the service: $1,017,990 USD for Twillio's phone verification service vs $887,069 USD for Amazon's web-hosting service (https://projects.propublica.org/nonprofits/display_990/824506840/02_2021_prefixes_81-83%2F824506840_201912_990_2021022217742945).

Peer-to-peer communication confers a lot of metadata resistance. There is no central server handling every message to which metadata can be exposed. It is harder for adversaries trying to mass-collect metadata about communications than to monitor traffic going in and out of known central servers. And there is no single point of failure. As long there is a route across the internet for you and your friend to connect, you can chat.

**Synchronicity**

There's an important thing to note about peer-to-peer communication: because there is no central server to store and relay messages, *you and your friend both need to have the app running and online in order to exchange messages.* Because of this, these PET apps are biased towards synchronous communication.

What if you bike across town to deliver a letter to your friend and… they're not home!? If you truly want to be peer-to-peer you have to hand deliver the letter directly to your friend. You can't just leave it for them (there is nowhere safe enough!). You must be able to directly reach your friend to deliver the message – this is the synchronous aspect of peer-to-peer communication.

Phone calls are also a good example of synchronous communication. You can't have a phone conversation unless you are both on the phone together at the same time. But who actually makes phone calls anymore? These days, we are much more accustomed to a mix of synchronous and asynchronous messaging, and centralized communication services like Signal are great for this. Sometimes you and your friend are both online and exchange messages in real time, but more often there is a long delay in between messages back and forth. At least for some people… some readers probably have their phone on and within reach at all times, and respond to every message they receive immediately, at all hours of the day. For them, all communication is and should be synchronous… you know who you are.

Switching to synchronous-only text communication can be a real shock at first. Some readers might remember what this was like from using AIM, ICQ, or MSN Messenger (if you remember these, your back hurts). You need to be conscious of whether or not someone is actually online. You can't fire off a bunch of messages if they are offline, to be delivered later. If either of you don't just keep the app running and online at all times, you and your friend might get into the habit of setting dates to chat. This can be really *nice.* Paradoxically, the normalization of asynchronous communication has resulted in an expectation to be basically online and responsive at all times. Synchronous communication encourages an *intentionality* to our communications, restricting it to times when we are actually online, instead of the expectation to be spontaneously available more or less all the time.

Another important consequence of the synchronicity of peer-to-peer connections: it can make group chats a little weird. What if not everyone in the group is online at the same time? Briar and Cwtch each handle this problem differently, so

that will be broken down in each app's respective section.

## Tor

Although peer-to-peer communication is very metadata resistant and avoids other pitfalls of using a central server, on its own it does not protect against "Big Data" metadata collection and traffic analysis. Tor is a very good mitigation for this, and PET apps route all traffic through **Tor**.

If you an anarchist reading this, you should already be familiar with Tor and how it can be leveraged to provide anonymity.[28] PET apps form direct peer-to-peer connections to exchange messages *through* Tor. This makes it much, much harder for any adversary, either one observing you in a targeted way or one trying to observe and correlate activity across the internet, to identify who is talking to who or make any other useful determinations. It's much harder to link a given user of a *pet* app to a real-life identity. All any observer can see is that you are using Tor.

Tor is not bulletproof, and potential issues with Tor or attacks on the Tor network are possible. Getting into the details of how Tor works would take up too much space here, and there are many resources online to teach you.[29] Understanding the general caveats to using Tor is also important.[30] Like Signal, Tor traffic can also be disrupted by interference at the level of internet infrastructure, or by Denial of Service attacks which target the entire Tor network.[31] It is still much harder for an adversary to block or disrupt Tor than it is to take down or block the central Signal Server.

It must be noted that in some situations, using Tor can single you out. If you are the only one using Tor in a particular region or at particular times, it can stand out. But this can be true of any uncommonly-used app. Having Signal on your phone also used to make you stand out. The more people using Tor the better, and if used correctly Tor provides better protection against attempts to identify users than not. PET apps use Tor for everything, by default, in a fairly foolproof implementation.

## No phone, No Problem

An easy win. Both the PET apps profiled here do not require a phone number to register an account. Your account is generated locally on your device and the account

[28] Or perhaps more accurately unlinkability: https://code.briarproject.org/briar/briar/-/wikis/FAQ#does-briar-provide-anonymity

[29] If you are not familiar with how Tor works, here's a gooe video: https://www.youtube.com/watch?v=QRYzre4bf7I

[30] Two good openers for this are https://tails.boum.org/doc/about/warnings/tor/index.en.html and https://www.whonix.org/wiki/Why_does_Whonix_use_Tor

[31] Tor reports on its current status around the world, indicating where there might be disruptions in the Tor network: https://status.torproject.org/

identifier is a very long random string of characters that you share with friends to become contacts. You can easily use these apps just on a computer, on a phone without a SIM card, or on a phone but without linking directly to your phone number.

## General Caveats of PET apps

### The Leaky Status

Peer-to-peer communication inevitably leaks one particular piece of metadata: the online/offline status of a given user. Anyone you have added as a contact, or who you have trusted with your user id (or any adversary who has managed to obtain it) can tell if you are online or offline at any given time. This does not really apply to our threat model unless you are particularly careless with who you add as a contact, or for public facing projects that publish their user id. But is worth noting because sometimes you don't want that one friend you are avoiding to know you are online!

### One Account on One Device

When you open these apps for the first time, you create a password that is used to encrypt your user profile, contacts, and message history (if you opt to save it). This data remains encrypted on your device when you are not using the app.

Because there is no central server, you cannot sync your account across multiple devices. You can manually migrate your account from one device to another, like from an old phone to a new phone, but there is no magic cloud sync. Having a separate account on each device is an easy workaround that encourages compartmentalization. Not having to worry about a sync'd version on a central server (even if encrypted) or other device is also an advantage. It forces more intentional consideration of where your data is and how you access it rather than just keeping everything 'in the cloud' (a.k.a. someone else's computer). There is also no copy of your account data backed up in a third party server that will restore your account if you forget your password or lose your device. If it's gone, it's gone.

Recall that the only ways around all this are to either trust a central server with a copy of your contacts and social network, or to rely on another social network the way Signal uses your contact list of phone numbers. We should not be trusting a central server to store this information (even in an encrypted form), nor using something like phone numbers. The possibility of having to rebuild our social network from scratch is the cost of avoiding those security issues, and actually encourages a practice of maintaining and re-establishing trusted connections with our friends.

### Battery Life

Running peer-to-peer Tor connections means that this app has to be connected and listening all the time in case any of your friends send you a message. These apps can be pretty battery-hungry on older phones. This is becoming less and less of

an issue though, as the battery usage improves in general and phone batteries get better.

**Not iOS-friendly**

Neither of these apps run on Apple's iOS, mainly due to iOS being hostile to any app establishing peer-to-peer Tor connections. This is unlikely to change in the future (though not impossible).

# PETting Zoo

It's time to meet these PET apps. Both have excellent user guides that provide detailed information about how to use them, but here is a quick overview of how they each work, their features, and what using them is like.

## Briar

Briar website: https://briarproject.org/

Briar user manual: https://briarproject.org/manual/

**Background and Vibe Check**

Briar is developed by the Briar Project, which is a collective of developers, hackers, and Free Software enthusiasts, mostly based in Europe. Besides resisting surveillance and censorship, the larger vision of the project is to build communication infrastructure and tools to be used during a disaster or internet blackout. Obviously this vision is of interest to anarchists who find themselves in regions where there is a high potential for a partial or total internet shutdown during a rebellion, or where general infrastructure collapse may occur (i.e. everywhere). If the internet is down, Briar can sync messages over Wi-Fi or Bluetooth. Briar also allows easy sharing of the app itself directly with a friend. It can even form a rudimentary mesh network between peers, so some kinds of messages can hop from user to user.

Briar is open-source and also commissioned an independent security audit in 2013.[32]

- As of this writing, Briar is available for Android and the current version is 1.4.9.
- There is a beta desktop version available for Linux (current version 0.2.1.) although it is missing many features.
- Windows and macOS versions of the desktop client are planned.

[32] https://briarproject.org/raw/BRP-01-report.pdf

## Using Briar

### Basic Chat

Basic chat works great. Friends both have to add each other to be able to connect. Briar has a nice little interface to do this in-person where you scan each other's QR codes. But it can also be done at a distance by sharing user IDs (as a 'briar:// link'), or any user can "introduce" users within the app, allowing two users to become contacts with each other via their mutual friend. A little friction in how you add contacts can feel inconvenient, but consider how this model encourages better and more intentional practices around trust. Briar even has a little indicator next to each username to remind you how you "know" them (in person, via sharing links, or via an introduction).

At present, in direct chats you can send files, use emojis, delete messages, and set messages to automatically disappear after seven days. If your friend isn't online, you can write them a message and it will send automatically the next time you see them online.

### Private Groups

Briar's Private Groups are basic group chats. Only the group's creator can invite additional members, so Private Groups are very intentional, meant for a specific purpose. Private Groups support threading (you can reply directly to a specific message, even if it isn't the most recent message in a chat) but it's pretty crude. You can't send images in a Private Group, nor enable disappearing messages.

Because Briar's group chats are truly serverless, things can be a bit weird when not everyone in the group is online at the same time. Remember synchronicity? Any group message will be sent to all the members of a group who are online at the time. Briar relies on all the members of a group to relay messages to other members who are offline. If you missed some messages in a group chat, any one of the other members who *did* receive those messages can relay them to you when you are both online.

### Forums

Briar also has a feature called Forums. Forums work the same as Private Groups, except that any member can invite more members.

### Blog

Briar's blog feature is actually kind of cool? Every user by default has one Blog feed. Blog posts made by your contacts show up in your Blog feed. You can also

comment on a Blog post, or 'reblog' a Blog post from a contact so it will be shared with all your contacts (with your commentary) – it's a rudimentary social network that functions just on Briar.

**RSS feed reader**

Briar also has a built in rss feed reader which fetches new posts from news sites over Tor. This can be a great way to read the newest communiqué from your favourite sketchy anarchist counter-info site (which probably provides an rss feed, if you didn't already know!). New posts from rss feeds you have added show up in the Blog feed, and you can 'reblog' them to share with all your contacts.

**Get Meshy**

Briar does a lot of cool things to move messages around between contacts without any central servers. Similarly to how Private Groups sync messages between members without a server, Forums and Blogs are relayed from contact to contact. All your contacts can receive a copy of a Blog or Forum post even if you are never online at the same time – shared contacts transmit the message for you. Briar does not create a true mesh network where messages are passed via any other Briar users (which could provide an opportunity for an adversary to operate many malicious Briar accounts and collect metadata). Briar does not trust any of your messages with users for whom they are not intended. Instead, every user that is supposed to receive a message also participates in transmitting that message to others who are also meant to receive it, and only with their own contacts.

This can be especially useful to create a trusted communication network that works even if the internet is down. Briar users can sync messages over Wi-Fi or Bluetooth. You could walk to the local infoshop, see a few friends and sync a variety of Blog and Forum posts. Then you come home, and your roommates can sync with you to get the same updates from all your mutual shared contacts.

**Get Meshy**

Each instance of the app only supports one account. So you cannot have multiple accounts on the same device. This is not an issue if you are using Briar just to talk with a close group of friends, but makes it difficult to use Briar for multiple different projects or networks you would otherwise want to compartmentalize. Briar provides several security-based justifications for this, and a simple one is as follows: if the same device uses multiple accounts, it could theoretically be easier for an adversary to determine those accounts are linked, despite using Tor. If the caretaker and the ghost are never seen online at the same time, there's a good chance they are using the same cell phone for their individual Briar accounts. There are other

reasons, and also potential workarounds, but for now having multiple profiles on the same device is not supported.

The Briar protocol also requires both users to add each other as contacts, or be introduced by a mutual friend, before they can interact. This prevents publishing a Briar address to receive anonymous incoming messages, like if you wanted to publish your Briar user id to receive honest reviews about a write-up comparing different secure chat apps.

**Briar and Asynchronicity**

Users *really* like their asynchronous communication. The Briar Project is working on a Briar Mailbox, which is another app that could be run easily on an old Android phone or other cheap hardware. The Mailbox would essentially stay online to receive messages for you, and then sync to your primary device over Tor when you are online. This is an interesting idea. A single Briar mailbox could potentially be used by multiple users who trust each other, like roommates in a collective house, or regular patrons of a local infoshop. Rather than relying on a central server to facilitate asynchronicity, a small and easy-to-set-up server that you control is used to store incoming messages for you and your friends while you are offline. This is still in development, so how secure it would be (e.g. would stored messages or other metadata be sufficiently safe if the Mailbox was accessed by an adversary?) is not known and would have to be evaluated.

## Cwtch

Cwtch website: https://cwtch.im/

Cwtch handbook: https://docs.cwtch.im/

**Background and Vibe Check**

So the name… it rhymes with 'butch.' Evidently it's a Welsh word that means *a hug that creates a safe place.*

Cwtch is developed by the Open Privacy Research Society which is a nonprofit based in Vancouver. Cwtch's vibe could be described as 'queer Signal.' Open Privacy is very invested in building tools to "serve marginalized communities" and to resist oppression. They've also worked on other cool projects, like research for something called 'Shatter Secrets' designed to protect secrets against scenarios where individuals can be compelled to reveal a password (like a border crossing).

Cwtch is also open-source and its protocol is based in part on the earlier PET project Ricochet. Cwtch is a newer project than Briar, but its development has moved fast and new versions come out frequently.

- As of this writing the current version is 1.8.0.
- Cwtch is available for Android, Windows, Linux, and macOS.

### Using Cwtch

When you first open Cwtch, you create your first profile, protected with a password. Your new profile gets a cute little generated avatar and a Cwtch address. Unlike Briar, Cwtch supports multiple profiles on the same device, and you can have multiple profiles unlocked at once. This is ideal if you want to have compartmentalized identities for different projects or networks without switching between multiple devices (but heed the potential security concerns of doing this!).

To add a friend, just give them your Cwtch address. You and your friend don't have to exchange addresses first to chat. This means with Cwtch you can publish a Cwtch address publicly and friends and critics can contact you anonymously. You can also set Cwtch to automatically block incoming messages from strangers.

Here's a Cwtch address to contact the author of this writeup with feedback or hate mail:

`g6px2uyn5tdg2gxpqqktnv7qi2i5frr5kf2dgnyielvq4o4emry4qzid`

In direct chat, Cwtch features some nice rich text formatting, emojis and replies. Each conversation can be set to 'save history' or 'delete history' when Cwtch is closed.

This is the barebones and it works great. At present, all of Cwtch's other features are "Experimental" and you can opt-in to them in the settings. This includes group chats, file sharing, sending photos, profile pictures, image previews and clickable links with link previews. Cwtch development has been moving pretty fast, so by the time you are reading this, all these features may be fully developed and available by default.

### Group Chats

Cwtch also offers Group Chats as an "Experimental Feature." Cwtch currently uses *user-operated* servers to facilitate Group Chats, which is very different from Briar's approach. Open Privacy considers metadata-resistant group chats to be an open problem, and hopefully from reading this far you can understand why. Similar to how the Signal Server operates, Cwtch servers are designed such that the servers are always considered 'untrusted' and learn as little as possible about message contents or metadata. But of course these servers are operated by individual users rather than a central third party.

Any individual Cwtch user can become the 'server' for a Group Chat. This is great for single-use Group Chats where a user can become the 'host' for a meeting or quick discussion. Cwtch Group Chat servers also allow asynchronous message delivery, so a group or community can operate their own server continuously as a service to their members.

How Cwtch approaches group chats is still under development and could change in the future, but it's a very promising and cool solution right now.

### Cwtch and Asynchronicity

Group Chats in Cwtch allow asynchronous messaging (as long as the server/host is online), but like Briar, Cwtch requires both contacts to be online for direct messages to be sent. Unlike Briar, Cwtch will not let you queue up messages to send to a contact when they come online.

### Cwtch's Crypto Caveat

In late 2019, Open Privacy, who develops Cwtch, received a $40,000 cad no-strings donation from the Zcash foundation. Zcash is another privacy-centric cryptocurrency similar but decidedly inferior to Monero.[33] In 2019, Cwtch was in very early development, and Open Privacy did some exploratory experiments around using Zcash or similar blockchain cryptocurrencies as creative solutions to various cryptographic challenges, with the idea that it could be incorporated into Cwtch at some point.[34] Since then, no further work with Zcash or other cryptocurrencies has been associated with Cwtch, and it seems to not be a priority or area of research for Open Privacy. But it must be mentioned as a potential red flag for people who are highly wary of cryptocurrency schemes. Recall, Signal already has a fully functional cryptocurrency built right into the app allowing users to send and receive MobileCoin.

# Conclusions

## "...has left the group"

Many readers may be saying to themselves "PET apps don't seem to support group chats very well... and I love group chats!" Firstly, who truly loves group chats? Secondly, it's worth bringing up critiques of how anarchists end up using group chats in Signal to make the point that the way they are implemented in Briar and Cwtch shouldn't be a dealbreaker.

Signal, Cwtch, and Briar all allow you to easily have a real-time (synchronous!) group chat for a meeting or quick collective discussion which could not otherwise happen in person. But when people refer to a "group chat" (especially in the context of Signal) this is not usually what they mean. Signal group chats often become huge, long running feeds of semi-public updates, shitposts, re-shared links, etc, that in practice are more like social media. There are more members than could realistically be having a functional conversation, let alone making decisions. The decrease in

[33] Zcash's creator, a wild guy name Zooko Wilcox-O'Hearn seems bent on ensuring Zcash is private but can't be used for crime!

[34] https://openprivacy.ca/blog/2019/12/03/Incentivizing-Trustlessness-ZcashFoundation-Donation/

utility and security with the increase in size, scope, and persistence of Signal groups was well-discussed in the excellent piece "Signal Fails".[35] The farther a group chat strays from small, short-term, intentional and single-purpose, the harder it is to implement with Briar and Cwtch – and this is not a bad thing. If anything, Briar and Cwtch promote healthier and more secure habits, lacking the 'features' of Signal that facilitate group chat dynamics critiqued in pieces like "Signal Fails."

## Proposal

Briar and Cwtch are both new projects. Some anarchists have already heard of them and are trying to use one or the other for specific projects or use-cases. Current versions might seem more cumbersome to use than Signal, and they suffer from the network effect – everyone is using Signal, so no one wants to be using something else.[36] It's worth pointing out that the apparent barriers to using Cwtch and Briar right now (still in beta, network effect, different than what you are used to, no iOS version) are all exactly the same barriers that discouraged people early on from using Signal (aka TextSecure!).

Getting people to learn and start using any new tool is difficult. Especially when the current tool they are used to seems to work just fine! There's no denying the challenge. This guide has ended up pages and pages long in an effort to make a convincing argument that anarchists, who possibly care the most about these issues, should try using these PET apps.

Anarchists have previously been successful at adopting challenging new electronic tools, spreading them, and wielding them effectively during acts of struggle and resistance. Normalizing the use of PET apps in addition to, or instead of, Signal for electronic communication will boost the resiliency of our communities, and of those we can convince to use these tools. They will help protect us from increasingly powerful metadata collection and analysis, insulate us from being reliant on a centralized service, and provide easier access to anonymity.

So here is the proposal. Having read this guide, implement it and share it. You cannot try Cwtch or Briar alone, you need at least one friend to try them with. Install them together with your crew and try using one or the other for a specific project that fits. Have a weekly meeting with people who can't meet in person to discuss news that was otherwise being shared in a sprawling Signal group chat. Keep in touch with a few far-away friends, or a crew that has been split up by distance. You don't have to (and probably shouldn't) delete Signal, but at the very least you will be helping build resilience by establishing back-up connections to your networks. As things are heating up, the likelihood of the type of intense repression or societal fractures that disrupts Signal in other countries is becoming

[35] https://north-shore.info/2019/06/02/signal-fails/

[36] Do you have a moment to talk about interoperability and federation? Maybe later?

more likely everywhere, and we will be well-served by having our back-up comms in place sooner rather than later!

Briar and Cwtch are both under active development, by anarchists and people sympathetic to our goals. By using them, either seriously or for fun, we can contribute to their development by reporting bugs and vulnerabilities, and inspiring their developers to push on, knowing that their project is being used. Perhaps even some of the more computer-inclined among us can contribute directly, by auditing their code and protocols or even joining their development.

Besides reading this guide, actually trying to use these apps as a collective of curious users is the best way to appreciate how they are structurally different from Signal. Even if you cannot bring yourself to use these apps regularly, trying different secure communication tools and *understanding* how and why and how they are different from what you are familiar with will improve your digital security literacy. You do not have to master the challenging math that underpins Signal's double-ratchet encryption protocol,[37] but better knowledge and understanding of how these tools work in theory and in practice leads to better operational security overall. As long as we are relying on infrastructure to communicate, we should be trying to understand how that infrastructure works, how it protects us or makes us vulnerable, and actively exploring ways to strengthen it.

### Final Words

This entire discussion has been about secure communication chat apps that run on our phones and computers. The final word must be a reminder that as much as using tools that encrypt and anonymize online communications can protect you against adversaries, you should still never type or say anything into any app or device without appreciating it could be read back to you in court. Meeting with your friends, face-to-face, outdoors and away from cameras and other electronics is by far the safest way to have any conversation that needs to be secure and private. Turn off your phone, put it down, and go outside!

## Appendix: some other apps you may have heard of

### Ricochet Refresh

https://www.ricochetrefresh.net/

Ricochet was a very early desktop PET app funded by the Europe-based Blueprint for Free Speech. Ricochet Refresh is the current version. Fundamentally

[37] For a great resource for understanding the Signal Protocol: https://www.redshiftzero.com/signal-protocol/

it is very similar to Cwtch and Briar, but is quite rudimentary – it features basic direct chat and file transfer, and only runs on MacOS, Linux and Windows. It's functional, but barebones, and has no mobile apps.

## OnionShare

https://onionshare.org/

OnionShare is a fantastic project that runs on any desktop computer and comes packaged with Tails and other operating systems. It makes it easy to send and receive files or have a rudimentary ephemeral chat room over Tor. It is PET too!

## Telegram

Telegram is basically Twitter. Having a presence there can be useful in certain scenarios, but it shouldn't be used for any secure communications and it leaks metadata everywhere. Spending more time critiquing Telegram is probably not useful here, but it shouldn't be used where privacy or security is desired.[38]

## Tox

https://tox.chat/

Tox is similar project to Briar and Cwtch, but it doesn't use Tor– it's just **PE**. Tox could be routed through Tor manually. None of the apps developed for Tox are particularly user-friendly.

## Session

https://getsession.org/

Session is worth addressing at some length. The vibe is very libertarian-free-speech-activist. Session employs Signal's robust encryption protocol, is peer-to-peer for direct messages and also uses Onion routing for anonymity (the same idea behind Tor). However instead of Tor, Session uses it's own Onion routing network where a 'financial stake' is required to run a Service Node to make up the Onion network. Crucially, this financial stake is in the form of a cryptocurrency that is administered by the foundation that develops Session. The project is interesting from a technological standpoint, clever even, but it's a very 'web3' solution wrapped up in cryptobro culture. Despite all their posturing, their group chats are not built to be terribly metadata resistant, and large semi-public group chats are just hosted on centralized servers (and apparently overrun with right-wing cryptobros). Maybe if

[38] https://nitter.net/m_hoppenstedt/status/1532706414635978760#m

the blockchain prevails in the end this will be a good option, but right now it can't be recommended in good conscience.

## Molly

https://molly.im/

Molly is a forked version of the Signal client for Android. It still uses the Signal Server, but it provides a little bit of extra security and features on-device.