# Article Title: How Signal Walks the Line Between Anarchism and Pragmatism

Article Date and Author: Jul 23rd 2023, Kai Ye

Article Content:

For 20 years, the only way to really communicate privately was to use a widely hated piece of software called Pretty Good Privacy. The software, known as PGP, aimed to make secure communication accessible to the lay user, but it was so poorly designed that even Edward Snowden messed up his first attempt to use PGP to email a friend of Laura Poitras. It also required its users to think like engineers, which included participating in exceptionally nerdy activities like attending real-life “key-signing parties” to verify your identity to other users. Though anyone could technically use PGP, the barrier to entry was so high that only about 50,000 people used it at its peak, meaning that privacy itself was out of reach for most.

These days, to talk to a friend securely, all you have to do is download a free app. For a certain set, that app will be Signal. Snowden and Elon Musk have recommended it; it’s been name-dropped on big-budget shows like House of Cards, Mr. Robot, and Euphoria, and its users include journalists, members of the White House, NBA players, Black Lives Matters activists, and celebrities trying to get their hands on Ozempic. Its founder has been profiled by The New Yorker and appeared on Joe Rogan’s podcast. A tiny organization with virtually no marketing budget has become synonymous with digital privacy in the public imagination.

Technology can be deeply shaped by the personal inclinations of a founder. Facebook’s light-fingeredness with user data is inseparable from its roots in Zuckerberg’s dorm room as an app for ranking women by their looks; Apple’s minimalist design was influenced by Jobs’ time spent practicing Zen Buddhism. Signal is no different. During its formative years, the charismatic face of Signal was Moxie Marlinspike, a dreadlocked anarchist who spent his time sailing around the world, living in punk houses, and serving free food to the unhoused. He led every aspect of Signal’s development for almost a decade, [at one point complaining](https://signal.org/blog/new-year-new-ceo/),  “I was writing all the Android code, was writing all of the server code, was the only person on call for the service, was facilitating all product development, and was managing everyone. I couldn’t ever leave cell service.”

In the field of cryptography, Marlinspike is considered the driving force behind bringing end-to-end encryption—the technology underlying Signal—to the real world. In 2017, Marlinspike and his collaborator, Trevor Perrin, received the Levchin Prize, a prominent prize for cryptographers, for their work on the Signal Protocol. Afterward, Dan Boneh, the Stanford professor who chaired the award committee, [commented](https://www.newyorker.com/magazine/2020/10/26/taking-back-our-privacy) that he wasn’t sure that end-to-end encryption would have become widespread without Marlinspike’s work. At the very least, “it would have taken many more decades,” he said.

The motivations that led to end-to-end encryption going mainstream lie far out on the political fringe. The original impetus for Marlinspike’s entry into cryptography, around 2007, was to challenge existing power structures, particularly the injustice of how (as he put it) “Internet insecurity is used by people I don’t like against people I do: the government against the people.” But sticking to anarchism would imply an almost certain defeat. As Marlinspike once [noted](https://moxie.org/stories/promise-defeat/), the “trail of ideas that disappears into the horizon behind me is completely and utterly mined over with failures … Anarchists are best known for their failures.”

For an idealistic engineer to succeed, he will have to build something that is useful to many. So there has also been an unusually pragmatic bent to Signal’s approach. Indeed, in many interviews, Marlinspike has taken a mainstream stance, insisting that “Signal is just trying to bring normality to the internet.” Signal’s success depends on maintaining its principled anarchist commitments while finding a wide-ranging appeal to the masses, two goals that might seem at odds. Examining how the app navigates this tension can help us understand what might come next in Signal’s new quest to reach “[everyone on the planet.](https://www.theverge.com/23409716/signal-encryption-messaging-sms-meredith-whittaker-imessage-whatsapp-china)”

Released after WhatsApp  set the standards for messaging, Signal’s problem has always been how to keep up with its competition—a fine dance between mimicry (so as to seem familiar to new users) and innovation (to poach users from its competitors). Signal started off by copying WhatsApp's user experience, while at the same time pioneering end-to-end encryption, a feature that WhatsApp turned around and copied from Signal. Throughout this evolutionary dance, Signal has managed to maintain an unusual focus on the autonomy of the individual, a wariness of state authority, and an aversion to making money, characteristics that are recognizably anarchist.

Because a small fringe of cypherpunks, Marlinspike included, came to see cryptography as a way to remedy the imbalance of power between the individual and the state, Signal focused on getting end-to-end encryption on messages and calls absolutely right. With Signal, no one can read your messages. Amazon can’t, the US government can’t, Signal can’t. The same is true for voice calls and metadata: A user’s address book and group chat titles are just as safe. Signal knows basically nothing about you, other than your phone number (which is not mapped to your username), the time you created your account, and the time you last used the app. Your data can’t be sold to others or cause ads to follow you around on the internet. Using Signal is just like talking with your friend in the kitchen.

Because Signal is committed to retaining as little metadata as possible, that makes it hard for it to implement new features that are standard to other apps. Signal is essentially footing the cost of this commitment in engineer-hours, since implementing popular features like group chats, address books, and stickers all required doing novel research in cryptography. That Signal built them anyway is a testament to its desire for mass appeal.

Signal also pioneered features that gave individuals more autonomy over their information, such as disappearing messages (which WhatsApp later adopted) and a feature that let users blur faces in a photo (which it rapidly rolled out to support the Black Lives Matter protests). At the same time, Signal has garnered users' trust because its code is open source, so that security researchers can verify that its end-to-end encryption is as strong as the organization claims.

For the ordinary user, though, individual autonomy and privacy may not be as important. On WhatsApp, users accept that it will be very hard to figure out what exactly the app knows about you and who it might be shared with. Users’ information is governed by an ever-shifting labyrinth of grudging caveats and clauses like “we will share your transaction data and IP address with Facebook” and “we can’t see your precise location, but we’ll still try to estimate it as best as we can” and “we will find out if you click on a WhatsApp share button on the web.” WhatsApp is also closed-source, so its code can’t be audited. If using Signal is like talking in a friend’s kitchen, using WhatsApp is like meeting at a very loud bar—your conversation is safe, but you’re exposed, and you’ll have to pay for your place.

If you’re not an anarchist, you may be less worried about a shadowy state and more worried about actual people you know. People in your community might be harassing you in a group chat, an abusive ex might be searching your chats for old photos to leak, or your child might have gotten access to your unlocked phone. WhatsApp’s features better support a threat model that is sensitive to interpersonal social dynamics: You can leave groups silently, block screenshots for view-once messages, and lock specific chats. WhatsApp can even view the text of end-to-end encrypted messages that have been reported by a user for moderation, whereas Signal has no moderation at all.

Idealists have called centralization one of the main ills of the internet because it locks users into walled gardens controlled by authoritarian companies. In a great stroke of pragmatism, Signal chose to be centralized anyway. Other encrypted-messaging apps like Matrix offer a federated model akin to email, in which users across different servers can still communicate through a shared protocol. (Someone on Gmail can still email someone on Yahoo, whereas someone on Facebook Messenger can’t contact someone on Signal.) This federated approach more closely mirrors anarchy; it could theoretically be better, because there would be no single point of failure and no single service provider for a government to pressure. But federated software creates a proliferation of different clients and servers for the same protocol, making it hard to upgrade. Users are already used to centralized apps that behave like Facebook or Twitter, and email has already become centralized into a few main service providers. It turns out that being authoritarian is important for maintaining a consistent user experience and a trusted brand, and for rolling out software updates quickly. Even anarchism has its limits.

What Signal has accomplished so far is impressive. But users famously judge software not on how much it can do, but on how much it can’t. In that spirit, it’s time to complain.

Because of Signal’s small team, limited funding, and the challenges of implementing features under end-to-end encryption, the app bafflingly lacks a number of important features. It doesn’t have encrypted backups for iOS; messages can only be transferred between phones. If you lose your iPhone, you lose all your Signal chat history.

Signal also doesn’t do a good job serving some of its core users. Activists and organizers deal with huge amounts of messages that involve many people and threads, but Signal’s interface lacks ways to organize all this information. These power users’ group chats become so unwieldy that they migrate to Slack, losing the end-to-end encryption that brought them to Signal in the first place. It’s common to try and make multiple group chats between the same people to manage all their threads. When users are hacking “desire paths” into your interface to create a new feature, or leaving because of the lack of the feature, that’s a strong hint that something is missing.

WhatsApp and Telegram, on the other hand, are leading the way on defining how group chats can scale up. WhatsApp “communities” gather different private group chats in one place, better mimicking the organization of a neighborhood or school that may be discussing several things at once. Telegram’s social media “channel” features are better for broadcasting info en masse, though Telegram’s lack of moderation has been blamed for attracting the kind of fringe crowd that has been banned from all other platforms.

It's no exaggeration to say that small features in a chat app encode different visions of how society should be organized. If the first reacji in the palette was a thumbs down rather than a heart, maybe we would all be more negative, cautious people. What kind of social vision did Signal arise from?

“Looking back, I and everyone I knew was looking for that secret world hidden in this one,” Marlinspike admitted in a 2016 [interview](https://www.wired.com/2016/07/meet-moxie-marlinspike-anarchist-bringing-encryption-us/). A key text in anarchist theory describes the idea of a “temporary autonomous zone,” a place of short-term freedom where people can experiment with new ways to live together outside the confines of current social norms. Originally coined to describe “pirate utopias” that may be apocryphal, the term has [since been used](https://www.documentjournal.com/2020/08/better-living-through-anarchy-tracking-the-rise-of-the-temporary-autonomous-zone/) to understand the life and afterlife of real-world DIY spaces like communes, raves, seasteads, and protests. And Signal is, unmistakably, a temporary autonomous zone that Marlinspike has spent almost a decade building.

Because temporary autonomous zones create spaces for the radical urges that society represses, they keep life in the daytime more stable. They can sometimes make money in the way that nightclubs and festivals do. But temporary autonomous zones are temporary for a reason. Over and over, zone denizens make the same mistake: They can’t figure out how to interact productively with the wider society. The zone often runs out of money because it exists in a world where people need to pay rent. Success is elusive; when a temporary autonomous zone becomes compelling enough to threaten daytime stability, it may be violently repressed. Or the attractive freedoms offered by the zone may be taken up in a milder form by the wider society, and eventually the zone ceases to exist because its existence has pressured wider society to be a little more like it. What kind of end might Signal come to?

There are reasons to think that Signal may not be around for very long. The nonprofit’s blog, meant to convince us of the elite nature of its engineers, has the unintentional effect of conveying the incredible difficulty of building any new software feature under end-to-end encryption. Its team numbers roughly 40; Marlinspike has just [left the organization](https://twitter.com/signalapp/status/1669374296785928193). Achieving impossible feats may be fun for a stunt hacker with something to prove, but competing with major tech companies’ engineering teams may not be sustainable for a small nonprofit with Marlinspike no longer at the helm.

Fittingly for an organization formerly led by an anarchist, Signal lacks a sustainable business model, to the point where you might almost call it anti-capitalist. It has survived so far in ways that don’t seem replicable, and that may alienate some users. Signal is largely funded by a big loan from a WhatsApp founder, and that loan has already grown to $100 million. It has also accepted funding from the US government through the Open Technology Fund. Because Signal can’t sell its users’ data, it has recently begun developing a business model based on directly providing services to users and encouraging them to donate to Signal in-app. But to get enough donations, the nonprofit must grow from 40 million users to 100 million. The company’s aggressive pursuit of growth, coupled with lack of moderation in the app, has already led Signal employees themselves to [publicly question](https://www.theverge.com/22249391/signal-app-abuse-messaging-employees-violence-misinformation) whether growth might come from abusive users, such as far-right groups using Signal to organize.

But there are also reasons for hope. So far, the most effective change that Signal has created is arguably not the existence of the app itself, but making it easy for WhatsApp to bring Signal-style end-to-end encryption to billions of users. Since WhatsApp’s adoption, Facebook Messenger, Google’s Android Messages, and Microsoft’s Skype have all adopted the open source Signal Protocol, though in milder forms, as the history of temporary autonomous zones would have us guess. Perhaps the existence of the Signal Protocol, coupled with demand from increasingly privacy-conscious users, will encourage better-funded messaging apps to compete against each other to be as encrypted as possible. Then Signal would no longer need to exist. (In fact, this resembles Signal’s original theory of change, before they decided they would rather compete with mainstream tech companies.)

Now, as the era of the global watercooler ends, small private group chats are becoming the future of social life on the internet. Signal started out a renegade, a pirate utopia encircled by cryptography, but the mainstream has become—alarmingly quickly—much closer to the vision Signal sought. In one form or another, its utopia just might last.