Phreeli:
An Early Analysis

Updated January 2026

Phreeli[1] launched as a new wireless service in December 2025, promising significant privacy and security improvements on other providers. The goal of this analysis is to evaluate whether activists, organizers, and other people facing government repression should use Phreeli in the immediate future.

The information available

Evaluating brand new tools can be difficult: we can't look to past behavior, we can't compare past audits to current performance, and we can't even look at customer service complaints to spot trends. The information available about Phreeli at time of writing is limited to:

- Phreeli's website and marketing materials
- Phreeli's sub-reddit (currently containing 11 posts, although there appear to have been additional posts requesting support that have been since deleted)
- A handful of articles from tech news sites (the most in-depth of which is behind Wired's paywall[2])
- A few posts on community and personal sites that amount to speculation

1 https://www.phreeli.com/
2 https://www.wired.com/story/new-anonymous-phone-carrier-sign-up-with-nothing-but-a-zip-code/

An in-depth analysis of Phreeli just isn't possible yet. Most potential users concerned about privacy and security likely should wait to use any new wireless provider until external audits and other data are available. However, an initial analysis of these materials and of materials relating to people involved in the company does have value, both for identifying possible concerns Phreeli may face moving forward and to consider the trustworthiness of Phreeli as an organization.

The network

Phreeli offers fairly standard wireless plans, including unlimited calls and texting, along with data. But the company doesn't have its own cellular network or towers: it's reselling T-Mobile's wireless services (as well as services from other providers such as NetworkIP / Elite Telecom). T-Mobile works with a variety of resellers known as mobile virtual network operators (or MVNOs), as do the other large wireless providers[3]. Other MVNOs include providers like Cricket Wireless, Google Fi, and Mint Mobile[4]. As an MVNO, Phreeli's startup costs are likely in the seven figures. If the company had instead attempted to build out its own network from scratch, the costs would be at least a hundred times higher, so acting as an MVNO is a logical business decision. As a result,

3 https://en.wikipedia.org/wiki/Mobile_virtual_network_operator

4 https://en.wikipedia.org/wiki/List_of_mobile_virtual_network_operators_in_the_United_States

though, Phreeli's users are subject to T-Mobile's terms of service, as well as those of other third-party providers Phreeli works with.

While practical from a cost perspective, Phreeli's status as an MVNO means that T-Mobile will always have access to certain kinds of information about Phreeli's users, as may the other service providers Phreeli works with. In order to connect a call or a text from or to a mobile phone, the network has to have certain information, such as the phone's number and location[5], which are logged as Phreeli's privacy policy notes[6]. That information, combined with users' phone numbers, is generally enough to track users[7].

And that's not the only information a mobile phone provides[8]. Using mobile apps leaks data in a number of ways and a variety of companies capitalize on connecting information from apps with information from wireless providers, for purposes ranging from advertising to political repression[9]. All this information is accessible to data brokers and law enforcement offers without needing even a user's name and payment details.

---

5 https://kiledjian.com/2025/12/17/in-the-final-weeks-of.html
6 https://www.phreeli.com/privacy/policy
7 https://arstechnica.com/tech-policy/2025/08/t-mobile-claimed-selling-location-data-without-consent-is-legal-judges-disagree/
8 https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data
9 https://www.eff.org/deeplinks/2026/01/ice-going-surveillance-shopping-spree

There's a good chance that Phreeli's promised privacy will face regulatory threats in the near future. Industry experts have suggested that MVNOs should expect increased enforcement for Know Your Customer regulations for eSIMs, requiring companies to be able to provide more user information to law enforcement[10]. Some industry analysts even suggest that the launch of Phreeli and other similar services could spur new regulations requiring wireless providers implement identity verification[11]. However, predicting future regulatory changes in the MVNO space is complicated by the existence of Trump Mobile, an MVNO likely operating on T-Mobile's network launched in mid-2025[12], as well as other factors which have increasingly politicized the FCC (which is responsible for regulating MVNOs) since the beginning of 2025[13]. It's especially difficult to predict if Phreeli's founder will be an asset in regulatory wrangling, given that Nicholas Merrill is perhaps best known for his multi-year lawsuit against the FBI and US Department of Justice related to the USA PATRIOT Act in the early 2000s.[14]

10 https://hwglaw.com/2025/02/07/client-advisory-on-the-fccs-enforcement-of-the-know-your-customer-rule-against-telnyx/

11 https://www.wirelessdealergroup.com/post/phreeli-mvno-launches-with-zip-code-only-sign-up-privacy-focused-wireless-service-and-what-it-means

12 https://www.fierce-network.com/wireless/trump-mobiles-made-america-phone-still-mia

13 https://en.wikipedia.org/wiki/Federal_Communications_Commission#Attempted_abandonment_of_independence_by_FCC_chairman_Brendan_Carr

14 https://en.wikipedia.org/wiki/American_Civil_Liberties_Union_v._Ashcroft

The data

So how does Phreeli plan to counteract this data collection? The company's marketing materials focus on plans to collect as little information about users as they possibly can, as well as separating account details (like names and payment details) from the information necessary to actually place calls (like phone numbers and locations).

The company's core claim is that users need only a zip code to sign up, with no need for an address, although this claim is misleading. Phreeli only clarifies that all users must provide not a zip code but a ZIP+4 code in its terms of service[15] and during the actual sign-up process. The US Post Office uses ZIP+4 codes to identify specific addresses within the larger zip code; it's functionally equivalent to providing a full address in most cases[16]. In practice, users can sign up without providing a name or information beyond beyond their ZIP+4 code, as long as they use cryptocurrency to pay for their service.

Phreeli also requires an address for users requesting hardware SIM cards. Users will be able get eSIMs via Tor in the future. That option may be a useful innovation for some users. However, Tor[17] isn't perfectly secure any more than

15 https://www.phreeli.com/terms-of-service
16 https://en.wikipedia.org/wiki/ZIP_Code#ZIP+4
17 https://en.wikipedia.org/wiki/Tor_(network)#Attacks_and_limitations

cryptocurrency[18] is. Both can be deanonymized and Phreeli has not indicated any steps the company may take to reduce such risks.

Phreeli also points to a cryptographic protocol they've named 'Double-Blind Armadillo' to prevent account information from being associated with a specific phone number[19]. According to a white paper written on Phreeli's behalf by Last Authority, the protocol will eliminate the need to connect a user's account details and the information necessary to connect calls. When a user pays their monthly bill through a system running this protocol, for instance, the payment system will generate a cryptographic token marking the account current without saving any information about the user. That token is then mixed in with other tokens and batch-processed to limit de-anonymization opportunities (like checking what tokens were issued at the same time given users made payments) before the entire batch of tokens is transmitted to T-Mobile or another wireless provider.

However, the white paper does not demonstrate a working version of this protocol, discuss what technologies are used to build it, or even say that the protocol has been implemented at all. Instead, the white paper states that, at time of launch, Double-Blind Armadillo is not in use. Initially,

18 https://www.cnet.com/personal-finance/crypto/are-cryptocurrency-transactions-actually-anonymous/

19 https://www.phreeli.com/files/PhreeliDoubleBlindArmadilloWhitePaper.pdf

Phreeli is using a less secure system that the white paper describes as “an acceptable level of security and privacy” despite marketing materials suggesting otherwise[20].

Assuming Double-Blind Armadillo is ever fully implemented, this approach will only protect a limited amount of user data. That’s true even for users who pay with cryptocurrency and use eSIM cards obtained via Tor in brand new phones that are purchased anonymously and only used to call other users taking the same precautions[21]. Protection will be more limited for a user who uses a phone they transferred from another wireless provider, ports over their existing phone number, logs into accounts associated with their name on their phone, or plays mobile games with ads. Users without the technical skills to use Tor and cryptocurrency may also struggle with setting up a Phreeli account without leaking data somewhere along the way.

Of course, as there are so far no audits of Phreeli’s implementation of any protocols or infrastructure, there’s no way to know that Phreeli’s systems actually provide even limited protection. Such audits can take significant time to prepare and may not be available for months.

---

20 https://www.youtube.com/watch?v=zLOXsFmLayw
21 https://www.phreeli.com/privacy/policy

The key players

Without access to more details about Phreeli's operations, potential users have to decide whether they trust the people behind the wireless startup.

Nicholas Merrill: The founder of Phreeli is the only individual named on the company's website. His resume includes founding Calyx Internet Access (an ISP) in 1995 and cofounding the Calyx Institute (a non-profit focused on digital privacy)[22] in 2010, as well as filing the first constitutional challenge against gag orders under the USA PATRIOT Act in 2004. Merrill left the Calyx Institute in August 2025, as part of a series of changes that led the organization to cease offering CalyxOS[23].

Louis Rossmann: While not listed on Phreeli's website, Rossmann posted a video announcing the launch of Phreeli and mentioning that he is a board member[24]. He is also listed on a 2024 SEC form detailing transfer of shares in Phreeli[25] Rossmann is an advocate for consumer rights, especially the right to repair, as well as the owner of an independent computer repair business founded in 2007. He operates a popular YouTube channel on related topics and is involved with multiple non-profits[26].

22 https://calyxinstitute.org/
23 https://www.reddit.com/r/CalyxOS/comments/1mf74e3/a_letter_to_the_calyxos_community/
24 https://www.youtube.com/watch?v=e8SnNNq6MaI
25 https://www.sec.gov/Archives/edgar/data/2009536/000200953624000001/xslFormDX01/primary_doc.xml
26 https://en.wikipedia.org/wiki/Louis_Rossmann

Steve Gelmis: Gelmis is also listed on Phreeli's 2024 SEC paperwork as a director, though has not publicly announced ties to Phreeli. Gelmis is founded Public Interest Network Services / Public Interest Telecom in 1984[27].

Least Authority: The consultancy that developed Double Blind Armadillo is named in Phreeli's white paper describing the protocol. Least Authority has worked on projects around decentralized systems and security since 2011[28]. In 2015, the company spun off the Electric Coin Company to operate Zcash, a privacy-focused cryptocurrency[29].

Zooko Wilcox: The founder of Least Authority[30], Wilcox has spoken to multiple publications about Phreeli and can be assumed to have worked on Double Blind Armadillo. Wilcox also worked on Zcash, including a stint as the CEO of the Electric Coin Company, and remains active in the community[31].

Additional staff: Phreeli likely has around 10 staff members, although information is extremely limited. Two additional staff members are listed on the company's LinkedIn profile: Phil Weiss and David Moo[32]. Weiss lists a position as Phreeli's general counsel, along with operating his own law

27 https://pinsarchive.ejcg.net/about/management.html
28 https://leastauthority.com/about-us/
29 https://en.wikipedia.org/wiki/Zcash
30 https://leastauthority.com/about-team/
31 https://en.wikipedia.org/wiki/Zooko_Wilcox-O'Hearn
32 https://www.linkedin.com/company/phreeli/people/

firm and teaching part-time. Moo lists a position as Phreeli's director of operations and appears to have worked at Calyx Internet Access with Merrill.

Funders: A single angel investor seems to have provided most of Phreeli's $5 million in funding. When asked about the investor's identity by Wired reporter Andy Greenberg, Merrill declined to provide their name[33].

The lack of details about most of the people involved in Phreeli's operations is concerning. It's not surprising that people who care about privacy decline to be identified publicly — but doing so limits an organization's ability to build trust. Without information on who is funding Phreeli, outside evaluators can't even guess if those funders might make demands of the company that endanger its ability to function, let alone to keep users data private[34]. It's a known issue in the space — even Tor routinely has to address funding the project received from the US government in order to maintain users' trust[35] — which makes Phreeli's lack of transparency all the more noteworthy.

Addressing concerns around Phreeli from other security-focused projects is virtually impossible without the organization increasing its transparency. Since Phreeli's launch, makers of secure phone operating systems other than

33 https://www.wired.com/story/new-anonymous-phone-carrier-sign-up-with-nothing-but-a-zip-code/
34 https://startupwired.com/2025/08/04/why-most-series-a-rounds-are-financial-traps-for-founders/
35 https://blog.torproject.org/category/financials/

the Calyx Institute have leveled accusations at Merrill, as well as unnamed Phreeli co-founders[36] and discussed warning their own users against the company. Many of these concerns are tied to Merrill's exit from the Calyx Institute, which was part of a larger chain of events that dramatically reduced users' trust in CalyxOS and other offerings from the non-profit[37]. Most of the details around his departure are not publicly available. When one departure can start such a damaging chain reaction, though, it's reasonable to assume that the people involved need to consider how to better work within organizational structures in the future.

Worse, what information Phreeli offers can be seen as misleading. For instance, Phreeli recommends using privacy-focused cryptocurrencies such as Zcash or Monero, going so far as to mention them in the company's privacy policy, adding that "Zcash and Monero are in no way affiliated with Phreeli– please take the time to learn about these services before using them."[38]. While technically a correct statement, Least Authority's work with Phreeli makes complicates that claim, as Least Authority created and then spun off Zcash and Wilcox remains a Zcash advocate.

---

36 https://piunikaweb.com/2025/12/29/grapheneos-warns-users-against-privacy-first-carrier-phreeli-recommends-silent-link-esim-instead/

37 https://www.reddit.com/r/CalyxOS/comments/1qe2410/what_are_your_plans_for_regaining_trust/

38 https://www.phreeli.com/privacy/policy

Trustability

If you take Phreeli's claims of privacy at face value, the company's offerings seem impressive. If you dig deeper, however, you will find that Phreeli seems to be promising more than they can actually offer (at least at the time of offering). It's unclear how many of the privacy measures the company promises have actually been implemented. Worse, the company's marketing materials frame details in ways that are at best overly-generous and at worst are misleading.

Phreeli seems to be quickly building an organizational culture that limits information, as well as downplays users' concerns, perhaps best evidenced in the company's sub-reddit. At time of writing, the sub-reddit contains 11 posts. However, multiple posts have been deleted from the sub-reddit, though comments associated with those posts are still discoverable via the accounts that posted them. The company's moderator appears to follow a policy of deleting posts requesting support from the company's sub-reddit after users have connected with support through Phreeli's website. Reviewing four such posts since Phreeli's launch suggests that multiple users have struggled with accessing eSIMs while signing up for the service[39], information that may be useful for potential users considering signing up. This approach is not necessarily unusual for many startups as it can be seen as eliminating negative

39 https://www.reddit.com/user/Team_Phreeli/

comments, as well as reducing users' ability to search for common issues and solutions. Overall, the strategy reduces both transparency and trust, which is worrying to see in an organization already lacking in both.

More concerning is the response one poster received when asking about Phreeli's terms of service around forced arbitration and class action waiver clauses — clauses Rossmann is known for advocating against. When asked about these clauses in Phreeli's sub-reddit, Merrill replied personally, essentially saying that the company would never take advantage of these clauses: "We're a small business, just getting started - and our advisors explained to us the many ways our existence is threatened if we don't have this, so we put it in... we - just like our customers - are little guys. We don't want to void warranties, post-hoc change terms of sale on people in disadvantageous ways, or hold people in abusive contracts. We just don't want to get destroyed in the early stages of launching a new company by bad faith opportunists using lawfare to wipe us out."[40] Merrill's philosophy seems to be that users should trust him and his company to do the right thing in any given situation. But as Rossmann says in his video about Phreeli, "I don't believe in 'Trust me, bro.'"[41] Customers can't trust a company's leaders claiming they would never use a given

40 https://www.reddit.com/r/Phreeli/comments/1pr4hnb/forced_arbitration_and_class_action_waiver/

41 https://www.youtube.com/watch?v=e8SnNNq6MaI

clause, because those leaders may change their minds or be replaced. Merrill suggesting otherwise demonstrates either willful ignorance about the realities of running a business or a concerning lack of care about users' security in the long run.

Ultimately, Phreeli is asking users to take a lot on faith — and users should refuse. In the absence of any audit or other evidence that Phreeli has implemented any of its promised security measures, users have to assume that Phreeli is just another MVNO passing data along to its wireless provider with no protection. And when you consider the little information that is available about the organization, its technology, and its staff, there's reasons to worry that Phreeli may even be worse than the average MVNO:

- a significant mismatch between marketing materials and terms of service demonstrates a willingness to deceive users
- an organizational culture of avoiding transparency endangers users' ability to access the services they pay for
- promising protection via technology that currently doesn't exist creates a false sense of security for users
- a founder whose departure impacted one organization's ability to continue operations could do the same again and leave users stuck

At this time, potential users should pass on Phreeli, especially if privacy and security are key concerns.

tl;dr

Activists, organizers, and individuals facing government repression should not use Phreeli. Even if Phreeli fully implements their proposed Double Blind Armadillo protocol, the company would need to address significant concerns around transparency and trustability to be considered a useful option for individuals looking to protect their privacy.